NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DOCUMENT-BASED MESSAGE-CENTRIC SECURITY USING XML AUTHENTICATION AND ENCRYPTION FOR COALITION AND INTERAGENCY OPERATIONS

by

Jeffrey Scott Williams Sr.

September 2009

Thesis Advisor:	Don Brutzman
Second Reader:	Don McGregor

This thesis was done at the MOVES Institute
Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
September 2009

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE Document-Based and Message-Centric Security Using XML Authentication and Encryption for Coalition and Interagency Operations

5. FUNDING NUMBERS

6. AUTHOR Jeffrey Scott Williams Sr.

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME AND ADDRESS
Naval Postgraduate School, Modeling Virtual Environments and Simulations Institute, Monterey, California 93943

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT

Different agencies and different nations are not able to securely communicate and share structured information due to differences in security policies and data formats. The current evolution of security and data policies is not solving this fundamental problem. Document-based message-centric XML security can provide satisfactory security within a diversified communications framework between traditional and nontraditional partners by utilizing existing Web standards for XML canonicalization, XML digital signature, XML compression and XML encryption. Vulnerabilities related to the exchange of cryptographic technologies are minimized by strictly adhering to open-standards technology. This approach thus resolves multi-partner trust challenges in regards to using another entity's equipment, software, or policy requirements through the proper adoption of standards-based structured data and alternative cryptographic algorithms. Exemplar results demonstrated in this thesis show that XML Security is a feasible approach for operations that include multiple agencies and coalition partners.

Alternative solutions are also available using proprietary technologies, but such approaches lock participants into commercial contracts, prohibit distribution and provide suspect capabilities. Therefore, they cannot attain interagency or international acceptance. Such methods involve the use of unique or proprietary message formats with customized encryption and compression algorithms that are not available for broad scrutiny by open source communities. Closed approaches cannot gain group trust.

This thesis specifically investigates XML standardization methods for various categories of unclassified data to provide secure information exchange among a wide audience, e.g. multi-agency task force or multinational coalition partners. Using an XML document-centric approach is a helpful organizing principle for this problem that provides levels of security consistent with common business practices achieved, within the constraints of the respective organizational security policies of each participant. The resulting design patterns for XML document development enhance confidentiality, integrity, and authentication commensurate with the nature of the unclassified document generated, while maintaining information objects at an appropriate level of security and acceptable level of risk.

14. SUBJECT TERMS Extensible Markup Language (XML), Extensible Markup Language for Transformations (XSLT), Extensible Markup Language Security, Extensible Markup Language Encryption, Extensible Markup Language Digital Signature, Extensible Markup Language Authentication

15. NUMBER OF PAGES
229

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

THIS PAGE INTENTIONALLY LEFT BLANK

DOCUMENT-BASED MESSAGE-CENTRIC SECURITY USING XML AUTHENTICATION AND ENCRYPTION FOR COALITION AND INTERAGENCY OPERATIONS

Jeffrey Scott Williams Sr.
Lieutenant Commander, United States Navy
B.S. Computer Science, Morehouse College, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
MODELING VIRTUAL ENVIRONMENTS AND SIMULATION (MOVES)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2009**

Author: Jeffrey Scott Williams Sr.

Approved by: Don Brutzman
Thesis Advisor

Don McGregor
Second Reader

Dr. Mathias Kölsch
Chair, MOVES Academic Committee

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Different agencies and different nations are not able to securely communicate and share structured information due to differences in security policies and data formats. The current evolution of security and data policies is not solving this fundamental problem. Document-based message-centric XML security can provide satisfactory security within a diversified communications framework between traditional and nontraditional partners by utilizing existing Web standards for XML canonicalization, XML digital signature, XML compression and XML encryption. Vulnerabilities related to the exchange of cryptographic technologies are minimized by strictly adhering to open-standards technology. This approach thus resolves multi-partner trust challenges in regards to using another entity's equipment, software, or policy requirements through the proper adoption of standards-based structured data and alternative cryptographic algorithms. Exemplar results demonstrated in this thesis show that XML Security is a feasible approach for operations that include multiple agencies and coalition partners.

Alternative solutions are also available using proprietary technologies, but such approaches lock participants into commercial contracts, prohibit distribution and provide suspect capabilities. Therefore, they cannot attain interagency or international acceptance. Such methods involve the use of unique or proprietary message formats with customized encryption and compression algorithms that are not available for broad scrutiny by open source communities. Closed approaches cannot gain group trust.

This thesis specifically investigates XML standardization methods for various categories of unclassified data to provide secure information exchange among a wide audience, e.g. multi-agency task force or multinational coalition partners. Using an XML document-centric approach is a helpful organizing principle for this problem that provides levels of security consistent with common business practices achieved, within the constraints of the respective organizational security policies of each participant. The resulting design patterns for XML document development enhance confidentiality, integrity, and authentication commensurate with the nature of the unclassified document generated, while maintaining information objects at an appropriate level of security and acceptable level of risk.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3D	Three Dimensional
AAV	Amphibious Assault Vehicle
AVCL	Autonomous Vehicle Command Language
BWC	Battle Watch Captian
C14N	Canonicalization
C2	Command and Control
C2IEDM	Command and Control Information Exchange Data Model
CENTRIXS	Combined Enterprise Regional Information Exchange System
CISR	Center for Information Systems Security Studies and Research
COE CMP	Common Operating Environment Common Message Processor
COI	Contact of Interest
COSMOS	Coalition Secure Management and Operations System
CUI	Controlled Unclassifed Information
CSS	Cascading Style Sheet
CSV	Comma Separated Value text file format
CWID	Coalition Warrior Interoperability Demonstration
DAC	Discretionary Access Control
DEM	Data Exchange Mechanism
DIS	Distributed Interactive Simulation protocol
DIS-XML	Distributed Interactive Simulation using Extensible Markup Language
DNS	Domain Name System
DOCTYPE	Document Type Definition

DTD	Document Type Definition
EXI	Efficient XML Interchange Compression
HTML	Hypertext Markup Language
IA	Information Assurance
IMT	Information Management Tool
IAW	In accordance with
JC3IEDM	Joint Consultation, Command, and Control Information Exchange Data Model
JITC	Joint Interoperability Test Command
KML	Keyhole Markup Language
MAC	Mandatory Access Control
MIP	Multilateral Interoperability Program
MOVES	Modeling Virtual Environments and Simulation
NPS	Naval Postgraduate School
OR	Operations Research
OTAT	Over-the-Air Transmission
OWL	Web Ontology Language
PDU	Protocol Data Unit
PII	Personally Identifiable Information
PKC	Public Key Cryptography
PKI	Public Key Interchange
RBAC	Role-based Access Control
RDF	Resource Description Framework
RPG	Rocket-Propelled Gernade
SAML	Security Assertion Markup Language

SAVAGE	Scenario Authoring and Visualization for Graphical Environments
SIGINT	Signals Intelligence
SGML	Standard Generalized Markup Language
URL	Uniform Resource Locator
VPN	Virtual Private Network
W3C	World Wide Web Consortium
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language
XML-MTF	XML-based Message Text Format
XKMS	XML Key Management Specification
XSBC	Extensible Schema-based Binary Compression
XSLT	Extensible Stylesheet Language for Transformations

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Through Christ all things are possible. Therefore, I give thanks to God for giving me the opportunity and perseverance to complete this work.

To my principal advisors Don Brutzman and Don McGregor, congratulations and thank you for successfully transferring your knowledge and skill sets that resulted in this student’s ability to complete a scholarly product with the focus on a real world problem. This product may be further developed and seen throughout the fleet and international communities. It must be noted that MOVES thesis products are not created in vacuums and a great deal of support through instruction and recommendations came from the Naval Postgraduate School Center for Information Systems Security Studies and Research (CISR) as Operations Research (OR) and the Modeling Virtual Environments and Simulations (MOVES) Institute itself. Within the MOVES department there exist the Scenario Authoring Visualization for Advanced Graphical Environment (SAVAGE) team that spend a great deal of effort in developing tools that were pertinent to my thesis. Mike Bailey and Terry Norbraten refined several tools within the X3D-Edit software suite as well as addressed several technical questions related to implementation. I’d also like to thank the thesis processors whom led me on a path to a successfully formatted thesis. Without the input and guidance of the NPS faculty from various disciplines, the concepts embodied in this thesis would not be a fully developed product worthy of Naval Postgraduate School.

Lastly, I am extremely grateful for the support and understanding of my wife, Natasha, and children: Jayla-10 Jeffrey Jr.-8 Samyra-6 and Christian-2. Having spent several weekday nights and weekends on school grounds, their unwavering devotion and faith in my ability to accomplish the mission with the promise that time will be spent with them was greatly appreciated. At times they inquired if I was actually on shore duty or another version of sea duty. God Bless them. Their support was critical to my pursuit of academic excellence embodied within this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND PROBLEM STATEMENT

A. INTRODUCTION

As the global migration from the industrial age to the information age continues, the world is becoming a more network-centric environment with an increased requirement for the exchange of information. However, the leaps in technology are not limited to those entities that collect and use it ethically. Unethical users, industrial spies, and criminal organizations plunder and siege the opportunity to steal and/or alter information in transit for their own nefarious purposes. Executive Order (EO) 13356 and 13388 called for improved sharing of information (Bush 2004, 2005A). However, current and future requirements extend the mandate beyond national security. The requirement is to be able to establish an interoperable framework that facilitates secure exchange of data communications between traditional and non-traditional partners over possibly insecure networks. Therefore, security policies that have existed for physical documents must be updated to include sufficient protocols and methods to protect electronic documents. The security policy and associated implementation at a minimum need to address in transit document support for non-repudiation, authentication, document integrity, and a level of confidentiality commensurate with the classification of the data being transmitted. These are issues that are faced in government, industry, and in consumer markets.

To combat these problems industry has developed several complex solutions, which may negatively impact the users computing experience to the point that policy may be ignored or warnings go unnoticed. Behavioral change is the most common quoted solution; however, the behavioral change manifests itself to both the operating system and the user. To enhance a safe and secure computing experience Dr. Phillip Hallam-Baker suggests that a human-systems integration approach to software design be undertaken by software developers in cooperation with the developers of security products such that the operating system innately takes a secure stance against infection and network infiltration (Hallam-Baker 2008A). Dr. Hallam-Baker addressed vulnerabilities facing users of the World Wide Web within “The DotCrime Manifesto: How to Stop Internet Crime” in which the following vulnerabilities were mentioned:

- Identity theft
- Masquerading (Spoofing) Attacks
- Hijacking
- Domain Name System (DNS) Security

In regards to identity theft he stated that the “…the real root cause is the inadequate authentication mechanisms used …” (Hallam-Baker 2008A) By embedding security within the document, personal identifiable information contributing to identity theft can be avoided because document fragments possessing such data can be encrypted. It is illegible to anyone who intercepted the document in transit or employed some other nefarious method without having access to the appropriate key to decrypt the data.

The motivation of this thesis is to show that existing web standards for document security can be commonly applied across a broad range of important scenarios by implementing XML Canonicalization (C14N), XML Authentication via digital signature, XML Compression and XML Encryption. This thesis also demonstrates a meaningful exemplar that can work for multiple agencies and nations.

The World Wide Web is not exempt from being vulnerable to attack. Originally it was not designed with security in mind, but much has been accomplished. Websites that reside on the web require protection from nefarious entities that would deface the site and/or redirect authorized users to alternate Web sites for the purpose of stealing personal data, services, financial information, or deny service to authorized individuals. When such problems occur, who is to be held accountable? Who should be held accountable: the attacked individual for lack of attention to detail, the corporation that owns the Web site for not implementing a more pronounced security symbology to emphasize protected content, the operating system and/or browser vendor, or a combination of all aforementioned? This is an argument for lawyers to hash out, but the average user does not care until they (or someone that they know) falls victim. Therefore, the issue becomes how to manage identity and clearly identify, document, and prevent users from falling prey without infringing upon the users browsing experience. Microsoft Windows

CardSpace, Verisign Labs Personal Identity Provider, and Security Assertion Markup Language (SAML) were developed to support identity management and mutual authentication (Hallam-Baker 2008A).

Information is a critical element of national power. This is stressed in “Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.” The elements of national power consist of diplomacy, intelligence, military, and economics (DIME). These elements are dependent upon each other to maintain an operational stable and effective nation. Since there is a global evolution to an information based society, U.S. interests include both civilian and national security systems. “The historic distinction between civilian agency systems and national security systems no longer serves the U.S. interest. Civilian agencies have not received the technical assistance they need to protect their systems in the current threat environment (CSIS 2008).” Hence, there is a closely coupled shared security need that is governed by policy as illustrated in Figure 1.

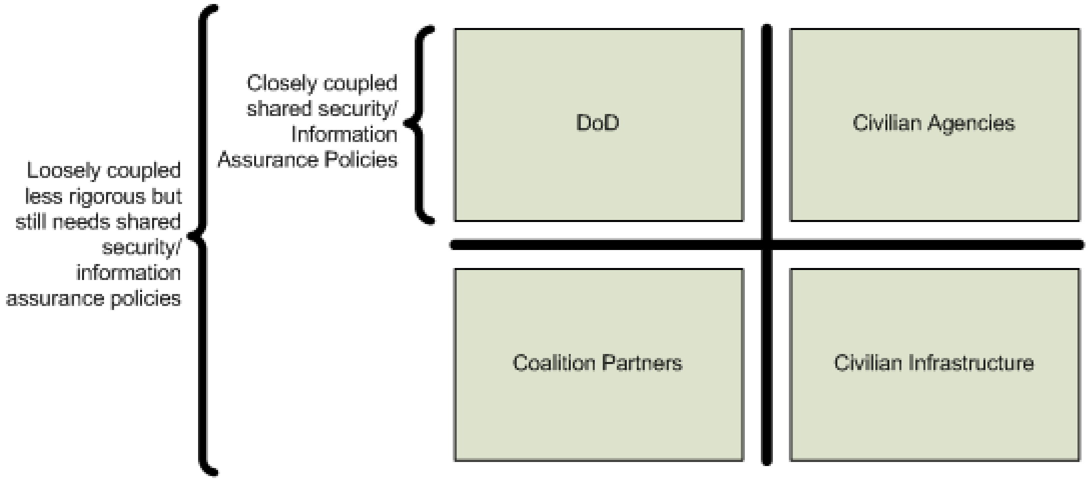

Loosely coupled less rigorous but still needs shared security/ information assurance policies
Closely coupled shared security/ Information Assurance Policies
DoD
Civilian Agencies
Coalition Partners
Civilian Infrastructure

Figure 1. This is a matrix depicting shared Information Assurance/ Security Policy needs across Department of Defense, Civilian Agencies, Coalition Partners and Civilian Infrastructure. (CSIS 2008)

A society that is connected globally can neither operate effectively in a vacuum cutting international ties, nor can it effectively protect itself by segmenting or dividing areas of responsibility and accountability. For certain cross-cutting problems, there must be common ground across all information domains to facilitate secure unclassified communications to flow between agencies. The degree of coupling of the shared policy between agencies differs by their trust relationships as illustrated in Figure 1. As nation efforts move to participate in international organizations where varying levels trust that exist amongst members, there is still a requirement to have a common ground in regards to sharing data to meet a common objective. Therefore, by implementing an international standard for security at the document level in which coalition partners supply their own tools and negotiate the base cryptography algorithm on scene, secure dynamic communications are possible. Additionally, an open standards-based technology solution is expected to be far more palatable to entities in attaining diplomatic concurrence from multi-agency/multination groups when entering a multilateral policy agreement on the technical aspects of communications. No one group would be seen as having an advantage over any other.

The Extensible Markup Language (XML) is a metalanguage that allows the creation of markup languages for arbitrary specialized domains and purposes (Geroimenko et al 2005). Therefore, based upon each participant's independent communication messaging structure, an extensible stylesheet transformation (XSLT) or other conversion tool can be used to adapt to their respective readable format to a common document structure, which thereby makes XML an extremely important tool. Additionally, with the proliferation and widespread use of mobile wireless devices within the business environment, XML is employed for greater flexibility. For example, examine a common object like a cell phone that not only sends and receives text messages but also enables web browsing. It is quite probabable that its using Wireless Markup Language (WML). However, with this comes a security concern that relate to ensuring ones personal and/or private information is protected. Who is to say that another entity is not standing by intercepting the transmission in a passive mode, using simple devices such as airsnort (Shmoo Group) or other with the combined use of a mobile phone sniffer (Elektor) and cellular phone interceptor? Therefore, requirements exist to guard against unauthorized access to information passed via voice or data networks. XML encryption and authentication can help to prevent data loss and disclosure to unauthorized parties, preserve document integrity during transmission, and provide of a means of non-repudiation through authentication.

With the popularity and integration of XML into major vendor's products, such as Sun/Oracle Systems OpenOffice Suite, Microsoft Office Productivity Suite, and numerous other commercial and open source tools, XML Encryption is a viable technology to support confidential communication exchange between parties that may transmit data over untrusted networks, such as the World Wide Web. Within the constraints of an organization's security policy, it may be necessary to establish point-to-point links with coalition participants. As such, there must be an avenue for the initiator to decide which parties are authorized to view the given data through a means called discretionary access control (DAC) as shown in Figure 2. DAC approach means that the keys to encrypt/decrypt or sign/authenticate documents are distributed on a discretionary basis, i.e. only shared among trusted participants.

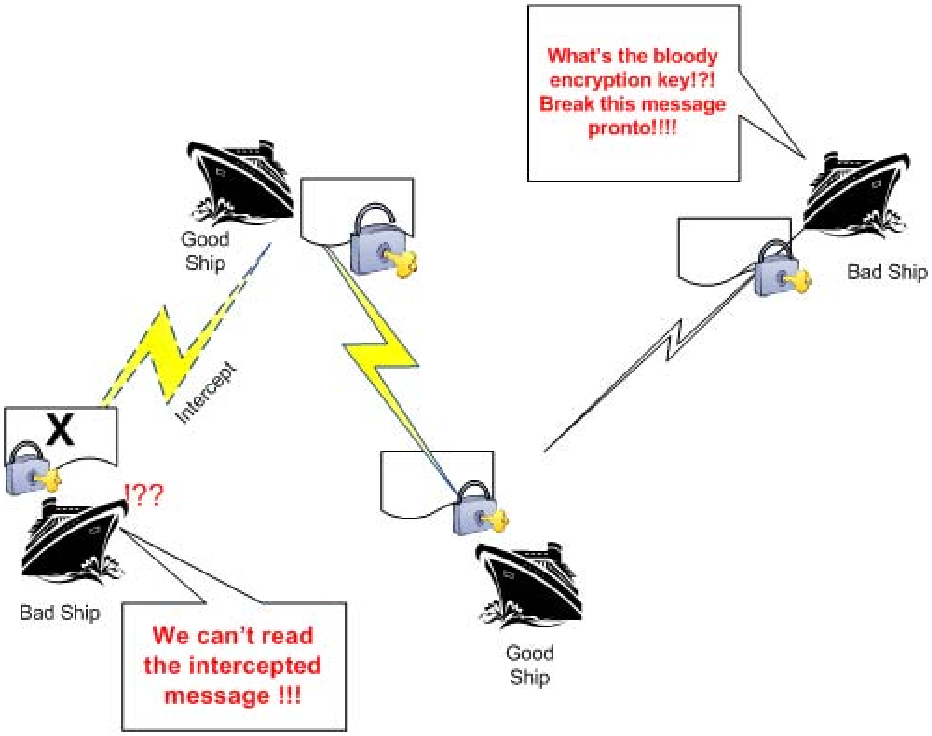

What's the bloody encryption key!?! Break this message pronto!!!!
Good Ship
Bad Ship
Intercept
X
!??
Bad Ship
We can't read the intercepted message !!!
Good Ship

Figure 2. Discretionary Access Control (DAC) of key distribution for encryption/decryption and signature authentication allows XML security to be applied at the document level. Restricting keys to trusted participants prevents unauthorized access to information

With the application of discretionary access control (DAC), the originator may send the document to multiple parties using a trusted or untrusted network. However, with XML encryption applied, only those participants that have the appropriate credentials can open it.

1. Thesis Goal and Scope Use tab key

Providing a framework for secure uncomplicated communications using XML encryption and authentication techniques employing discretionary access control (DAC) applied at the document level is the primary goal of this thesis. The thesis also explores the proper combination of Efficient XML Interchange (EXI) compression, XML digital signature, and XML encryption methods. Algorithms implemented are using open source tools such as Apache libraries and X3D-Edit (Brutzman).

The documents used and classification levels applied in this thesis are purely unclassified, which promotes collaboration with traditional and non-traditional partners with minimal exchange of hardware or cryptographic technology. All technology used is open source and freely available to the general public. There is an element of information assurance (IA) that briefly discusses elements of encryption, authentication, confidentiality, and integrity. Nevertheless it is assumed that any such documents originate in a secure enclave and is able to transit through a series of untrusted networks before reaching a trusted partner's secure enclave.

2. Security—How is it Defined within the Scope of the Thesis?

Security in the context used within this thesis refers to the four major tenents of information assurance which are defined as follows (CNSS Glossary Working Group):

- **Authentication** - Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
- **Confidentiality** - Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
- **Data Integrity** - Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

- **Nonrepudiation** - Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

The CNSS 4009 defines information assurance as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. This system does not explore network availability in regards to XML encryption and authentication.

It is assumed that other elements of security such as physical security, information security, etc. have been resolved for each secure-enclave endpoint and are thus beyond the scope of this thesis. This thesis does not address unauthorized physical access to the platform used to generate the document, nor does it address viral infections on either the host or destination machine. It is thereby assumed that point of origin and point of destination are secure and the network path by which the document is to arrive is insecure. This arrangement matches multiple agency or coalition-nation operations.

The suggestions and recommendations for implementing the encryption are derived from the World Wide Web Consortium (W3C) XML Encryption Working Group (W3C Working Group). Document-centric security enhances the security posture of an organization when properly implemented. Furthermore, it is designed to support the goals and objectives of existing organization security policy. It is not intended to replace existing measures or policies for classified information. Due care must be taken to properly implement document-centric security. Failure to adhere to the principles of due care may result in the compromise of a network-centric organization and other affiliated organizations to which it may be interconnected.

3. Methodology

The chapters explore XML encryption and authentication verifying that it is a viable option under multiple operating systems using various languages derived from XML and translated via a respective extensible stylesheet language transformations

(XSLT) using the Naval Postgraduate School's TrackDataConversionHub repository. Case studies explored in which this technology can be applied. This thesis also examines the ordering of events to determine the optimum sequence of checking for well-formed XML documents, validating document against a schema (as appropriate), processing the document to ensure that it is in canonical form, compressing the document using EXI compression, and finally processing the document using digital signature and encryption.

X3D-Edit version 3.2, Oxygen and XMLspy served as the primary tools for generating and processing XML data to show proof of concept for the developing framework (Brutzman 2009)(Altova 2009)(SyncRO Soft Ltd. 2009). Cases studies include an in-depth analysis of modeling secure attributes embedded at the document level that supports the establishment of dynamic communications in multi-agency Homeland Defense task force, civilian-military operation, multinational humanitarian assistance disaster relief, Civilian Joint & Coalition communications, and secure transmission of information through an untrusted network. Dynamic communications refers to the ability to construct and tear down a trust network utilizing DAC.

B. MEASURABLE SUCCESS GOAL

The methodology presented study provides a framework to pass unclassified structured data to multiple platforms, in a safe and secure fashion, from a secure point of origin via untrusted intermediate networks to its secure destination, utilizing standards-based approach to XML document-centric security.

Secure distribution of keys for encryption/decryption and signature authentication is left as future work. Interested readers are directed to the corresponding W3C Recommendation for Public Key Infrastructure (PKI) as one candidate for this approach. It is noteworthy that establishing a secure set of channels (as described in this thesis) for information transfer can also be used for secure distribution of key updates.

C. THESIS QUESTIONS

This work addresses the following questions.

1. Can an XML document that includes XML Encryption and XML Signature Elements provide adequate security commensurate with the security level of the data contained therein?

2. How can the use of XML encryption and authentication best assist in the confinement of data to trusted partners?

3. Do the standardized XML Signature, XML Encryption and authentication recommendations within the construct of Discretionary Access Control (DAC) satisfy Information Assurance (IA) requirements while transmitting or sharing data for which different gradients within the unclassified classification level for which each group of users are authorized to view?

4. Can an XML document or message fragment be restricted to showing the appropriate level of allowed data access by automatically checking the credential store local to the machine from which it is being accessed?

5. Do these techniques further apply when used in Web Services and real-time XML chat messaging, as well as X3D visualization and simulation streaming?

6. What role might Security Assertion Markup Language (SAML) play in concert with these document-centric design patterns?

7. Can document-level XML security be compatibly applied within the current and projected restrictions and best practices governing coalition and multiagency operations?

D. INITIAL CONSTRUCT

This thesis topic developed from talks with Don Brutzman about potential design of a prior program called Coalition Secure Management and Operations System (COSMOS), a system intended to facilitate collaborative information sharing among multinational military coalitions. By applying intent-based constructs to the Command and Control systems in current use, and by leveraging the Command and Control

Information Exchange Data Model (C2IEDM) as a sharing medium, COSMOS was intended to show the ability for multinational military coalition partners to cooperate and collaborate (CADS 2009). The initial system discussed is illustrated in the Figure 3.

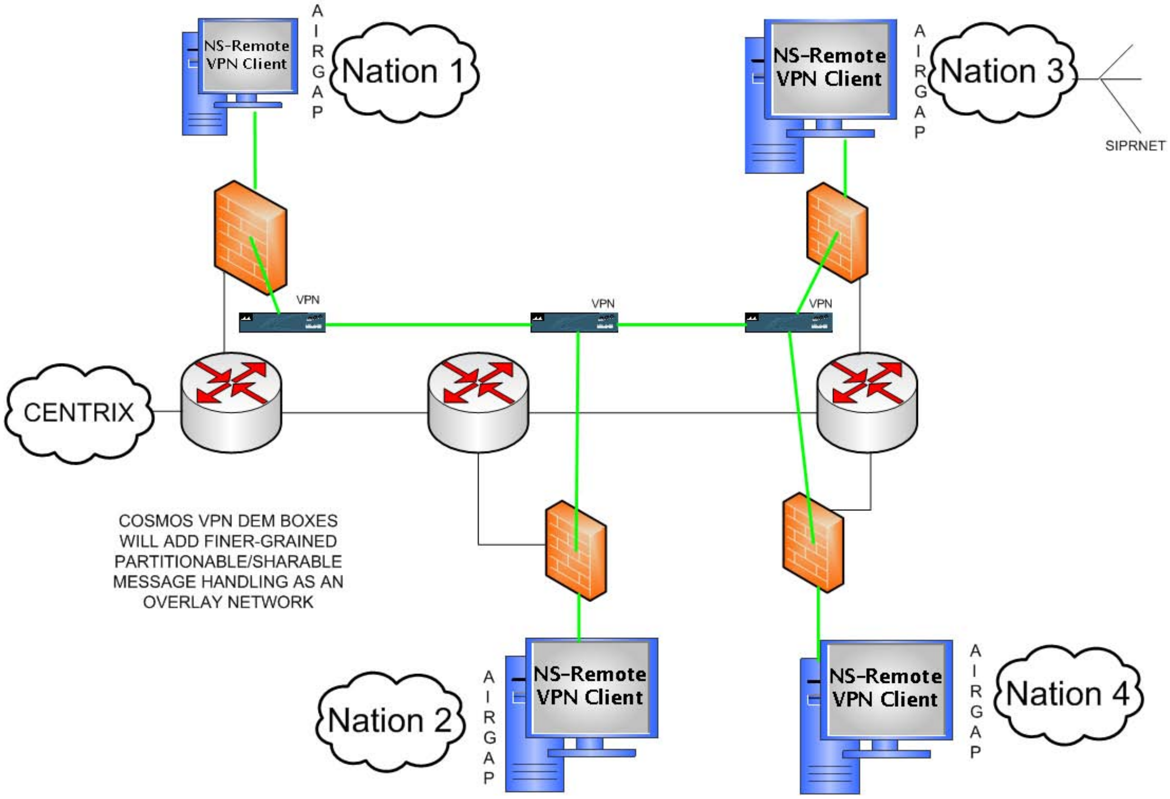


Figure 3. Design alternatives for the COSMOS program inpired the initial construct for the thesis. This architecture diagram shows secure sharing via trusted virtual private networks (VPNs).

In Figure 3 , there are four nation states (NS) that are exchanging information via COSMOS. Each nation has their own respective firewall such that the security policies of that particular nation are enforced. In other words only limited sharing is taking place between partners. To enhance security, each NS logs into a VPN in this manner data can flow between CENTRIXS and the respective NS. Each trusted VPN is overlayed on a shared network

Several fundamental problems exist with such an approach. Virtual Private Network (VPN) gateways are often implemented via proprietary software and/or hardware, which cannot be trusted by most partners. CISCO uses IPSEC, which is standards-based, but may have some proprietary parts (CISCO). A common network backbone is unlikely to be shared by all partners. Finally, compatibility or compliance with the security policies abd requirements of a notional network like CENTRIXS cannot be permitted (or agreed to) by ad hoc partnerships of agencies and nations. Thus, any framework architecture such as that shown in Figure 3 cannot scale up to accommodate a diverse set of participants.

In 2007, the Joint Interoperability Test Command (JITC) conducted an assessment on COSMOS. The assessment focused on interoperability objectives by providing data to and receiving data from external interfaces, as well as using standard communications ports, protocols, and data formats (Joint Interoperability Test Command 2007). Although COSMOS was able to demonstrate information exchange between coalition partners it experienced reliability and connectivity issues during the Coalition Warfighter Interoperability Demonstration 2007. For additional information detailing the final report visit JITC Web site at http://www.cwid.js.mil/public/CWID07FR/htmlfiles/314int.html.

Design requirements for COSMOS, nevertheless, establish the long-term needs with a realtime virtual environment to support communication coordination and cooperation across mixed untrusted network environments supporting varying levels of trust between participating organizations became apparent.

Another related effort was also inspired by the challenges facing the COSMOS program. Structured XML data is a core requirement for coherent information exchange among multinational parties. However, XML tends to be verbose compared to legacy protocols, and bandwidth throughput is limited. Due to XML’s verbose nature, XML documents must be compressed to be useful to coalition partners. There are multiple potential solutions to this issue. One early candidate solution was XML schema based binary compression (XSBC), a software algorithm to compress and decompress documents and images. However, XML documents must have a schema reference else XSBC cannot be used (xmsf.sourceforge.net)(Seren, 2003).

Given the broad requirement to establish shared security using XML documents and XML compression, this work focused on applying XML Encryption and Authentication within a framework that allows partners to share information across multiple information domains. For clarity and respectability, this thesis is focused solely on unclassified information. It explores alternatives that encourage multinational cooperation for joint and coalition operations by implementing an approach based on international standards to the broad challenge: Securely communicating with nontraditional entities to achieve a common goal.

E. THESIS ORGANIZATION

Chapter I provides a general overview of the thesis topic describing in general terms the scope of the thesis. It also provides the initial set of thesis questions that were posed during the thesis

Chapter II provides a summary of background knowledge with references that in order to understand the thesis.

Chapter III presents XML Security capabilities in regards to structure, XML key management, order of operations as well as a brief look at the individual operations required by XML Digital Signature and Encryption.

Chapter IV defines the overarching problem, summarized in 3 as follows:

Multinational/Multiagency communications between multiple actors within a heterogeneous networking environment employing discretionary access control via cryptographic key distribution.

- Navigation of multiple security and procedural frameworks to acquire secure communications over insecure medium.
- Providing secure embedded communications at the document level to enable multiple XML fragment access based upon cryptographic key.

Chapter V identifies several use cases and approaches to using efficient XML interchange compression with XML Digital Signature and Encryption. Some of the topics included in chapter V are:

- Application of XMPP Chat in relation to XML Encryption and Digital Signature

- Possibility of SAML Interactions with XMPP Chat
- Requirements for a basic XML message
- A brief exploration of the Basic XML Document Structure
- Approaches with EXI to include suboptimal, recommended, and ultimately a goal state for the application of EXI compression with XML security
- Application of XSLT translations to pass track data between two systems using dismiliar XML-based languages
- Document and Message Disemination Types in relation to Authenticity, Message Integrity, and Confidentiality

Chapter VI explores applications of technologies and looks at the possible integration of those technologies based upon ATALANTA and CTF 151 operations within the Gulf of Aden / Horn of Africa. This section explores the following:

- Preliminary steps prior to initiation of operations involving OPTASK COMMS
- Practical Encryption technologies
- Time to crack encrytion methodologies based upon key size.
- XML Security vulnerabilities

Chapter VII explores provides conclusions and recommendations

Appendix A explores a variety of naval MTF messages as well as illustrates sample data that was converted from a CSV to an XML file format.

Appendix B is contains a chart that takes a snapshot of 37 maritime leaders from around the world. This information is a synopsis of information contained in Proceedings March 2009 edition.

Appendix C contains and XSLT stylesheet that was taken from the NPS SAVAGE TrackDataConversionHub as of August 2009. The date is specified here as it is likely that the title and date of this archive may change several times as it evolves. Appendix D contains an overview of X3D-Edit's integrated security features that facilitate XML Verification and Validation, C14N, XML Digital Signature, XML

Encryption. XML EXI compression integration with X3D-Edit is mentioned briefly. It was released September 2009 hours prior to the finalization of this thesis.

II. RELATED WORK

A. INTRODUCTION

The Internet was originally developed to pass information between two end points. With technological improvement and the Web became easier to use and far more manageable. Therefore, Security of web-based information grew in importance. Hypertext Markup Language was one such catalyst that initiated social change and brought the web to public's desktop. However, the evolution of the Web as we know it today has its origins with the U.S. Department of Defense's Arpanet. It has enable the transition of official correspondence using Message Text Format systems. Those systems have evolved and XML messages can also be generated to enable commanders to communicate to an international audience. Though able to communicate, information must be safeguarded in in transit as well as storage similar to the manner in which documents are stored. As the number of documents increased, there must be some mechanism to ensure that documents of a certain type contain a common format. This is accomplished by the use of DTDs or Schemas. Their use assists in expediting the retrieval of documents by ensuring that they meet a defined format to establish validity. Throughout the evolution of the web, real time chat and the available technologies for controlling items remotely were a concern that were met with XMPP and DIS XML. To enhance the user experience X3D technologies were developed which brought a pleasant environment to engage in computer-based activities.

B. SECURITY OVERVIEW

The Internet was not initially designed with security in mind. It was designed to expeditiously share information between multiple networked computers. Security was an afterthought. Unlike brick and mortar organizations security safeguards utilizing procedures, security guards, physical vaults, and log sheets that exist for securing paper based documents and valuables are insufficient for electronic documents. The aforementioned protection mechanisms would be part of an organizational security policy. A security policy is documentation that is designed to enforce specific rules and or regulations to safeguard information, personnel and equipment. An information systems security policy is a statement that outlines how entities access each other, what operations different entities can carry out, what level of protection is required for a system or software product, and what actions should be taken when these requirements are not met (Harris, 2007). The policy outlines the expectations that the hardware and software must meet to be considered in compliance. This thesis focuses on a flexible generalized information systems security policy that provides protection of electronic data from unauthorized personnel.

In providing the level of protection warranted and guaranteeing authenticity, message integrity, and non-repudiation, one must sign a document. When a consumer purchases an item on credit he/she can endorse an IOU promissory voucher stipulating that he/she agrees to repay the organization that owns the card at a later date. Both the consumer and the retailer retain copies of the invoice. The signature is valid because no two people write exactly alike. If a payment is in dispute at a later date, the retailer can present the invoice that bears the signature and an arbitration authority or judge can verify that the signatures match. Therefore, non-repudiation, message integrity, and authenticity have been achieved. Since both the consumer and the retailer have copies of the receipt, the contents can be compared to verify the correctness of the charges agreed. A similar concept is applied to the digital world. Using XML digital signature, an entity or corporation can sign the document using their unique private key that can later be verified using their corresponding public key. XML digital signatures by design provide for authentication, message integrity, and non-repudiation (W3C XML Security Specifications Working Group 2008).

1. Mandatory Access Control (MAC) and Discretionary Access Control (DAC)

In particular, the interest lies in the passing of a document from a secure network to a secure network via an unsecured medium such that the document can only be accessed by a given individual possessing the corresponding cryptographic key.

Unsecured simply refers to the fact that the organizations system administrators lack the ability to control what takes place within the region. The message originator decides who is authorized to access the document and therefore encrypts either the entire or parts of the document with the appropriate key. This concept is known as discretionary access control (DAC) because it is not a protocol that determines access but the message originator. A system in which access is predetermined is known as mandatory access control (MAC). Using DAC, there is no firm system policy of who is entitled to a given key. The author determines to whom the key is sent. The recipient of the key is entitled to access to the information. DAC is handled by key distribution described in later chapters. However, it must be stressed that the originator's control is limited to whom he/she sends the document. Upon receipt, the recipient of the document has control over distribution of the document.

2. XML in 10 Points

XML is the language of choice for a variety of reasons. (Boss) "XML in 10 Points" delivers ten valid critical design points in support of the deployment of XML within an enterprise network. The 10 points are as follows:

- XML is for structuring Data
- XML looks a bit like HTML
- XML is text but isn't meant to be read
- XML is verbose by design
- XML is a family of technologies
- XML leads XML to XHTML
- XML is modular
- XML is new but not that new
- XML is the basis for Resource Description Framework (RDF) and Semantic Web
- XML is license-free, platform-independent and well supported.

It has evolved as an industry standard since 1998 and has steadily been adopted and integrated in several products and as part of information and technical educational curriculum throughout the country, which mitigates the risk of supportability. Being license-free and platform independent are another great boon because it enhances an organizations flexibility in regards to intellectual property rights, which in turn promotes information sharing between heterogeneous networks having dissimilar security policies (Boss 1999). The possibilities using XML are endless.

3. Encryption

Encryption is a method of representing human readable text (plain text) into a non-intuitive form by using an algorithm that manipulates the characters. The new text string that is formed is known as ciphertext. By encrypting the document, a degree of confidentiality is attained. The strength of the confidentiality is based upon the algorithm used and the key length. Further discussions on the strength of the algorithm are beyond the scope of this thesis. In this manner, anyone may receive or intercept the document, but only those with the corresponding cryptographic keys can open the document. An example of encryption is a sentence that each character has been transposed by 3 letters e.g. “the cow jumped over the moon” would read “wkh frz mxpshg ryhu wkh prrq” . Naturally, this algorithm can be swiftly broken and would only be sufficient for a child’s game. Today’s encryption algorithms such as blowfish, advanced encryption standard (AES), triple data encryption standard (3DES), etc., are far more advanced and would yield the level of protection required to transmit sensitive material with relative confidence that the contents would not be easily revealed.

C. BENEFIT OF STORED ENCRYPTED FILES

The secure exchange of electronic data has always been an area of concern. Current technologies may implement a electronic portal in which you log in and make a database query. However, such systems require the organization to grant limited access to their network. It may be via file transfer protocol (ftp), trivial file transfer protocol (tftp), telnet, etc. but either way the system is exposed to vulnerabilities such that a command shell can be created or the system later compromised. If files are encrypted at the document level, they cannot be accessed by personnel that do not have the corresponding key. Therefore, even if the system is compromised, the encrypted files continue to have a level of protection above those that are not encrypted. No file protection means that a brother Donald can read sister Duck's journal because she left herself logged on. However, if sister Duck is encrypts or even password protects the file, chances are that brother Duck, though curious, would not invest the time to continue to break into the file. He may have access to her system but not to the plaintext contents of her file.

D. THE TRANSPORT MEDIUM

The medium is the physical path by which a bit of data transits from one point to another. It consists of radio frequency (RF), copper wire, fiber optics, and even water. Drop a stone in a pail of water and you'll see ripples. Place an object in the path of those rips and you'll see the ripples go around the object. Data transmission is the same. You do not have control of the data once it leaves your network.

Similar to brother Donald and sister Duck, documents transmitted over the internet and radio frequency spectrum face similar issues. Both of these mediums are insecure. If two vessels, SS Bobmansky and USS McCloud, want to communicate with one another, they may send a low frequency message. However, since the HMS Scotts is also in the area, she may passively intercept the message. If the message is not encrypted then the content is not protected and therefore its availability extends the intended audience. For example, take the international soccer tournament in which Brazil and the UK are playing against each other. The SS Bobmansky, HMS Scotts, and USS McCloud are in the midst of a multinational exercise. The SS Bobmansky sends an unencrypted message to USS McCloud saying "Go Brazil!!! " Sports enthusiasts aboard the HMS Scotts passively intercept the transmission and are not very happy with the content. People that actively follow the teams are very passionate over their particular sport of choice. Although the described situation is benign the issue could have been avoided by simply encrypting the documents.

E. MESSAGE TEXT FORMAT (MTF)

The United States (U.S.) Message Text Format (USMTF) is a designed to provide a standardized format for the U.S. Department of Defense (DOD) and associated U.S. agencies to facilitate the exchange of information. Its format is governed by military standard (MIL-STD) 6040A Department of Defense Interface Standard U.S. Message Format Description. To provide interoperability amongst the services it requires its data to be well formed with a base structure. All messages have three common parts, which are heading, body, and ending. The heading contains introductory text including overall security classification, flag words, and special handling instructions. (Air Support Control Officer/ Air Support Operations Operator Course Student Handouts, 2008) The Defense Information Systems Agency (DISA) is the sponsor of the USMTF program and maintains the configuration management of the USMTF standard for the Department of Defense (DoD). USMTF enhances coalition warfighting effectiveness through the standardization of message formats, data elements, and information exchange procedures (Sullivan, 2006).

F. EXTENSIBLE MARK-UP LANGUAGE MESSAGE TEXT FORMAT (XML-MTF)

XML MTF is USMTF that is designed to utilize the World Wide Web. It uses structural notation that fully utilizes the power of native XML. Interoperability is provided through a common message syntax which can be processed by user systems through use of commonly available tools and techniques and can leverage future Web techniques. NATO formats addressed by the Standard Agreement (STANAG) 5500 Allied Data Publication-3 (AdatP-3) are also supported by XML-MTF via the XML-MTF Schema Generation Specification which serves as a point for converting standard MTF messages into W3C XML. The NATO Message Text Format Working Group (MTFWG) manages the STANAG 5500 ADat-P3. XML-MTF is currently supported by several products to include Common Operating Environment Common Message Processor (COE CMP), IRIS Message Formatting System (MFS), Turboprep, and various others. (DoD, 2003)

G. HYPERTEXT MARKUP LANGUAGE (HTML)

HTML is a language based on the Standard Generalized Markup Language (SGML) that allows graphic and text based data to be uploaded to the World Wide Web. It is a computer language for representing the contents of nonsequential writing inclusive of links, media, and text (Berners-Lee, 1999). Most web pages are written in HTML with a growing shift to extensible hytpertext markup language (XHTML) which is HTML following the stringent rules of XML which in turn improves structure and ensures that the file is valid and ready for parsing by any browser. HTML is perhaps the main reason why the popularity of the web has increased exponentially such that it is now a household term.

H. EXTENSIBLE MARKUP LANGUAGE DOCUMENT TYPE DEFINITION (DTD)

A DTD is a collection of rules that define the content and structure of a valid XML document (Carey 2007). XML files must either match a schema or a DTD. A file is checked against a DTD to ensure that it strictly adheres to the structure defined. If a file is found to be invalid, then an error occurs. The following is an example DTD embedded within an XML file.

```
<!DOCTYPE place (
   <!ELEMENT place (name, latitude, longitude, elevation)>
   <!ELEMENT name (#PCDATA)>
   <!ELEMENT latitude (#PCDATA)>
   <!ELEMENT longitude (#PCDATA)>
   <!ELEMENT ELEVATION (#PCDATA)>
]>
<place>
   <name>Cat City</name>
   <latitude>95.3</latitude>
   <longitude>138.6</longitude>
   <elevation>100</elevation>
</place>
```

Figure 4. An XML file must be valid and can be validated against a schema. The DTD portion starts with the "<!DOCTYPE" declaration.

The DTD is the only definition and validation mechanism embedded within the XML recommendation that facilitates the DTD to be embedded directly into an XML document (Ayers 2007).

I. EXTENSIBLE MESSAGE AND PRESENCE PROTOCOL (XMPP)

The Extensible Messaging and Presence Protocol (XMPP) is an open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data (XMPP.org). XMPP is used for instant messaging over the Internet. It is a form of middleware that does not rely upon a central server. Anyone can set up an XMPP server and host chat sessions. Several open source and proprietary organizations have implemented XMPP to facilitate collaboration. XMPP has several strengths:

- Decentralized Architecture-no single point of failure because anyone can run his/her own XMP server
- Open Standard-Formalized by the Internet Engineering Task Force, XMPP is an approved instant messaging and present technology under the RFC3920 and RFC 3921.
- Industry Support-XMPP has been implemented and vetted through several large organizations such that security tactics techniques and procedures exist to securely isolate XMPP servers from the public Jabber network. This facilitates communications on closed networks.
- Customizable-Additional functionality can be added to XMPP to ensure interoperability

Despite the strengths, the XEP-0024 Publish/Subcribe XMPP specification had a few drawbacks that include issues with scalability and presence data overhead. However, this was corrected with XEP-0060 Publish-Subscribe XMPP update (XMPP Standards Foundation).

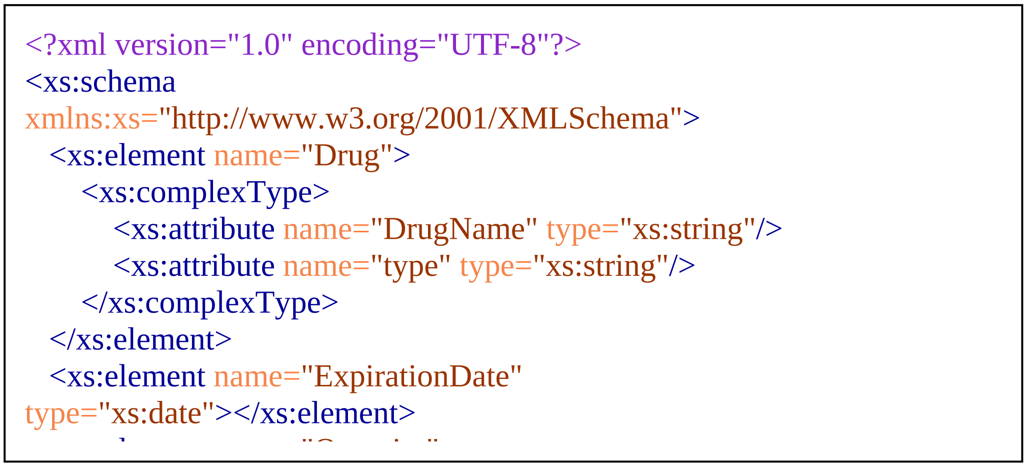
J. XML SCHEMA

An XML Schema is an XML document that can validate the content and structure of other XML documents (Carey 2007) . They fully support the W3C Namespace recommendation, and are created using basic XML. Schemas can be customized. A namespace provides a simple method for qualifying element and attribute names used in Extensible Markup Language documents by associating with namespaces identified by the internationalized resource identifiers (IRI) references (XML Core Working Group 2006). The XML Schema namespace name is http://www.w3.org/2001/XMLSchema. It contains all the vocabulary used to build a schema definition.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Drug" type="xs:string"/>
  <xs:element name="ExpirationDate" type="xs:date"/>
  <xs:element name="Quantity" type="xs:integer"/>
</xs:schema>
```

Figure 5. Schemas are written entirely in XML, and in turn validate the correctness of other XML documents.

XML schemas have two types of categories: simple and complex. Figure 6 above uses a simple datatype. A simple datatype is defined in the XML Schema using the empty element e.g. <xs:element name=”Drug” type=”xs:string”/> Simple types contain a single value. A complex type contains at least one value placed within a defined structure as in Figure 6.



```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Drug">
    <xs:complexType>
      <xs:attribute name="DrugName" type="xs:string"/>
      <xs:attribute name="type" type="xs:string"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="ExpirationDate"
type="xs:date"></xs:element>
```

Figure 6. Schemas can have combination of complex and simple types. The complexType is the element Drug which has two children DrugName and type.

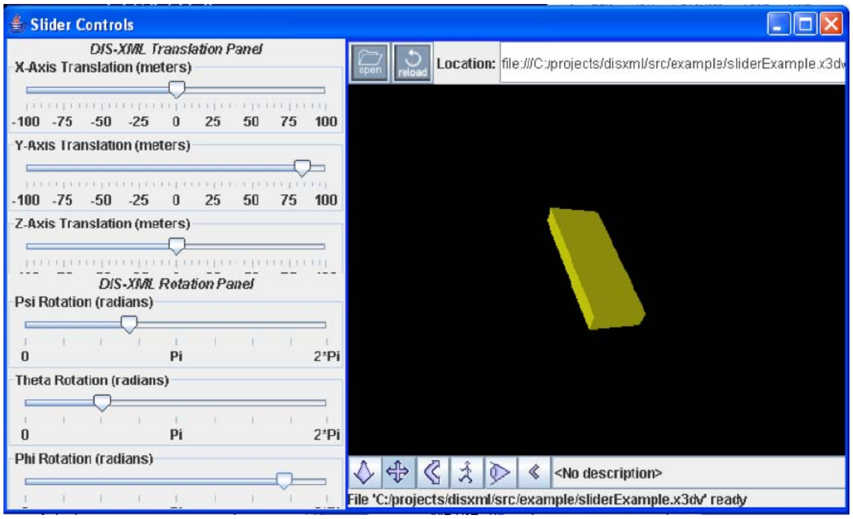
K. DISTRIBUTED INTERACTIVE SIMULATION (DIS XML)

Distributed Interactive Simulation is a binary standard for exchanging information in military simulations. Binary format Protocol Data Units (PDUs) are exchanged in order to update positions of entities in 3D virtual worlds. DIS XML represents the PDU in an XML format such that they can be read from the wire in a binary format, turned into Java objects, and then written out in XML format thereby enhancing the interoperable nature of the simulation. DIS XML is created using a combination of automatically generated code and hand written code. The features of DIS-XML include:

- The ability to read and write PDUs in XML format
- A simple networking framework
- An implementation that includes about twenty PDUs, and XML schema descriptions for about 30 more
- A slider application that allows the user to rotate an X3D box in a window using Yumetech's Xj3D libraries
- Ability to send and receive packets to Xj3D implementations
- A rudimentary JUnit test framework
- A modified BSD open source license
- An XML schema that describes much of the DIS protocol
- Some code that can be used in MATLAB to read and write PDUs

- An XMPP (jabber chat) bridge that passes XML-ified DIS PDUs across a chat channel
- Simple sender and receiver programs
- An ant build file

(Sourceforge Retrieved August 2009). The following is an example screen shot of XML-DIS in action using X3D-Edit.



Location: file:///C:/projects/disxml/src/example/sliderExample.x3dv

File 'C:/projects/disxml/src/example/sliderExample.x3dv' ready

Figure 7. XML and XML-DIS can be integrated in a number of tools. The screenshot above is taken from X3D-Edit tool DIS Console interface using Yumetech's Xj3D Browser plug-in (Blais 2006).

L. EXTENSIBLE 3D (X3D)

X3D is a royalty-free open source International Organization for Standardization (ISO) standard XML based file format and run-time architecture for representing and communicating computer graphics in 3D. "It is an initiative to leverage 3D as digital media as easily as we do with text and 2D graphics. It provides the technology to enable customers to view, modify, customize, and reuse 3D visualizations in other applications on the web or on any network device from cell phones to supercomputers. X3D is features a lightweight core 3D runtime delivery engine and is broadcast ready. It is well specified and runs in near real time. It is the successor of virtual reality markup language and is an absolute must to efficiently render graphics via web services, distributed networks, or cross platforms (Web3D.org).

M. EXTENSIBLE MARKUP LANGUAGE SCHEMA-BASED BINARY COMPRESSION (XSBC)

> XSBC is a library designed to compress XML documents and messages. It is designed to support both large documents like X3D and SVG files, as well as short messages such as SOAP and XML Remote Procedure Call (XML-RPC). A major feature of this library is the ability to register compressors for an attribute type, and element or document fragment. This allows data-aware compressor algorithms to get much better compression than typical generic routines. (Sourceforge)

N. EFFICIENT XML INTERCHANGE (EXI)

EXI is a potential successor to XSBC. It is currently in last call for the W3C and shall soon be an official recommendation. The W3C defines EXI as follows: “EXI is a very compact representation for the Extensible Markup Language (XML) Information Set that is intended to simultaneously optimize performance and the utilization of computational resources. The EXI format uses a hybrid approach drawn from the information and formal language theories, plus practical techniques verified by measurements, for entropy encoding XML information. Using a relatively simple algorithm, which is amenable to fast and compact implementation, and a small set of data types, it reliably produces efficient encodings of XML event streams (Efficient XML Working Group, 2008).” Sheldon Snyder, a graduate student in Modeling Virtual Environment and Simulations Program, is in the process of refining an EXI compressor in accordance with the specification. As of this writing the compressor is not online but it is expected to eventually be fully integrated into X3D-Edit. From preliminary test results, the EXI compressor appears promising. The results are display in the Table 1 .

Appendix A contains the messages that were compressed and contrasted using EXI compression and GZIP.

O. EXTENSIBLE STYLESHEET TRANSFORMATION (XSLT)

An XSLT is a method of converting data from one structure to another without changing the original data source. Unlike XSLT 1.0, which can only convert XML to XML, XSLT 2.0 has the potential of converting a comma separated file or other file format to XML via the use of regular expressions. Review the XSLT 2.0 specification for further information on XLST (XSL Working Group 2007).

P. SUMMARY

Due to the popularity of the Internet, security is a growing concern. Personal and business, and fiduciary data sent via the World Wide Web require some level of protection from theft, unauthorized modification, and unauthorized access. Some systems allow the user to specify who may access the information, whereas, in other systems, it is based upon a mandatory policy such as any user cleared to use the system may access the information which is a form of mandatory access control. Nonetheless, access control mechanisms alone are not enough. There must exist a method of verifying that the authenticity of the document. XML digital signatures perform this function in addition to message integrity verification and non-repudiation. Encryption covers the confidentiality piece of the pie by scrambling data. In regards to data, confidentiality, message integrity, authentication and non-repudiation are critical factors in regards to properly securing a document. Protecting the document from unauthorized access is accomplished via encryption. Digital signatures properly employed assist in the reassurance that the message is authentic, unaltered, and from a specific individual/entity. To mitigate the expense of the verbose nature of XML Encryption it is critical to employ some method of binary compression such as EXI. EXI compression assists pertinent data in reaching low-bandwidth communities in an expeditious fashion.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SECURITY-RELATED XML CAPABILITIES

A. INTRODUCTION

XML Security is a mature technology that enables financial transactions and transmissions of personally identifiable information via the World Wide Web. To this end there must be some measure to define what it means to be secure. By examining the Dolev-Yao model of security and the two party cascade models in addition to the XML Key Management Specification (XKMS) within the scope of XML security, an understanding of what it means to be secure is attained (Dolev and Yao 1983).

XML Security has several intermediary processes to ensure authenticity, message integrity, and confidentiality. Before any of these things can take place, the encryption algorithm must be negotiated between the clients such that keys can be exchanged appropriately. Thereafter, when both parties confirm that they can securely exchange data with the other then information exchange of data can take place. Each XML message must be checked to ensure that it is valid and well formed prior to being placed on the wire. Failure to perform checks generally result in a message-rejection error. XML Encryption provides confidentiality. The digital signature provides authenticity, and message integrity.

B. BASIC ANALYSIS OF PROTOCOLS

The organization is sending Controlled Unclassified Information (CUI) to many personnel at once. However, each participating organization employs a different set of protocols and methodology for sending and receiving and validating documents for both integrity and authenticity. Many other other organizations may join the group as time progresses. Some of the participants are permanent members of the group and others may remain for as long as it continues to focus on objectives that are mutually beneficial to the organization. The lead organization decided to use a standards-based approach using user datagram multicast protocol such that the messages are broadcast to participating group of internet protocol addresses. Based upon the transmission medium, there is a need to protect the content of the transmission against unauthorized access while providing a robust content without requiring major alterations of the participant's architecture. By employing XML Encryption and authentication at the document level, secure dissemination of material can be achieved.

Prior to deployment of the technology, it is critical to tailor the implementation to the lowest common denominator in terms of network capability when developing the architecture in regards to type of XML cryptographic technology to use. The more verbose the technology the more bandwidth consumed per transmission. Throughout this document E_x and D_x is used to represent the encryption keys. In order for a transmission to be secure, there must be an E_x for each D_x. This allows for asymmetric keys, symmetric keys, and Public Key Infrastructure.

Encryption is the conversion of plaintext such as "The Fox Jumped Over the Moon" to ciphertext such as "Yjr Gpc Ki,(rf Pbrt yjr <ppm". The algorithm used for decryption of the example given is simply using the key to the right of a standard QWERTY keyboard to denote the appropriate letter. However, usable encryption is far more sophisticated as to conceal the content of the data. Therefore, authentication, the process of determining that an entity is who they claim to be, is accomplished via encryption because it is assumed that in a utopian society that only the authorized parties have the appropriate keys to encrypt and decrypt the message.

This alone is not enough, there needs to be some mechanism in place to prove that the message was sent by an authorized entity and ensure that the message has not been compromised since its transmission. To achieve the verification of the sender's identity, a digital signature denoted by S_x … S_n is used. Depending upon the ordering of operations a digital signature can be used to ensure the integrity of operations on a document. A digital signature is an electronic signature specific to an individual or organization. It is mathematically computed and combines the hash of the document with the certificate of the user. A hash is a deterministic function that takes a variable-length block of data and returns a fixed-length bit string such that a change to the data changes the hash value (Schneier 1996). Given the following process from A → B would the message remain secure:

$$\begin{array}{ccc} A & & B \\ Encrypt(Digitally\ Sign_A(Document)) & \xrightarrow{E_Y S_Y(M)} & Decrypt(Verify\ Digital\ Signature(Document)) \end{array}$$

The transmission from A→ B is E_x D_x S_x ,which using the cascading two party protocol for simplicity would be secure because the E_x D_x reduces down to 1, which means that a key pair exists leaving only the digital signature. XML encryption is based upon the digital signature. This issue is discussed in more detail in later sections of this chapter.

This chapter examines the set of operations required to securely exchange information in which security is embedded at the document level. The operations required are verification of well formed XML, validation against a schema, XML canonicalization, digital signature, Efficient XML Interchange Compression (EXI), XML in generation of the document and the decryption, EXI decompression, XML validation, signature and integrity validation and finally display or rendering of the data within the recipient designated format and structure.

XML encryption can be used to encrypt Extensible Mark-up Language (XML) files and non- XML files (XML Encryption Working Group 2002). Document-centric security is ideal in situations requiring traditional and non-traditional partners to work in a cooperative manner to achieve a common objective. Multi-agency and multinational partners that form a task force requires flexibility such that XML and non-XML based content are passed securely via the same medium. Therefore, it is not uncommon for photographs, documents in other formats such as MS Word 2003 or Adobe Portable Document File (PDF) format to be exchanged between players. This thesis examines XML security applied against XML documents within an operational environment in further detail in later sections.

C. XML ENCRYPTION OPERATIONS

1. Key Management

Key management is an integral part of XML encryption. The exact operation is covered described in detail in the W3C XKMS Specification. It is necessary to have a key management framework in place to support dynamic messaging with participants that join the task force for a brief period as well as those entities that are semi-permanent partners. The base requirements for any key management program are the following:

- Time To Live (TTL) for any key within the system
- Nounce – a randomly generated number
- Type of system -- ring of trust or centralized methodology
- Key distribution mechanism

The following discussion presents a brief overview of details necessary to establish the exchange of cryptographic keys. To meet this objective, cryptographic key exchange between participating members is required. Key exchange falls into one of two different arenas: Symmetric in which keys are previously exchanged and Asymmetric in which key participants exchange keys. In regards to public key infrastructure (PKI), the Needham-Schroeder-Lowe (Fabrega 1999) protocol is used to illustrate the key exchange. For example, a new participant joins the task force and requires keys to participate in the exchange of data. Let us call this new participant entity B. Entity B sends a request to entity A encrypted with entity A's public key and a nonce (a randomly generated number). Entity A decrypts the message and sends back a nounce it generated in addition to entity B's nonce, as well as its identity. Entity A encrypts the message with B's public key. Entity B receives the message and sends entity A back its nonce encrypted with A public key.

In shorthand notation, the flow for Needham-Schroeder-Lowe protocol would be as illustrated in Figure 8:

Step 1.   B → A: $\{N_b, B\}_{KB}$

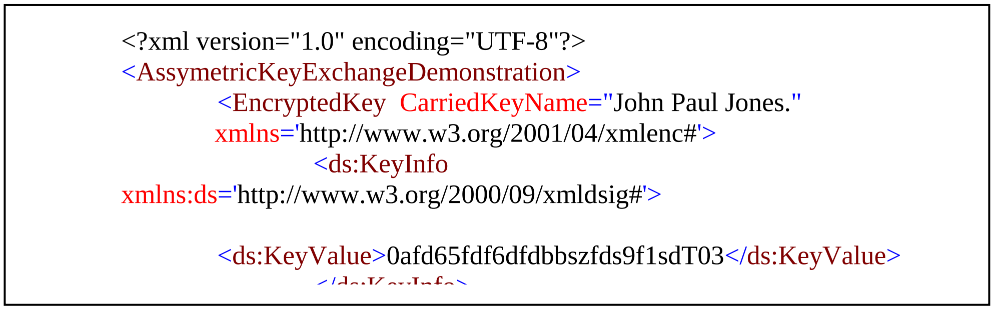
Step 2.   A → B: $\{N_b, N_a, A\}_{KA}$

Step 3.   B →A: $\{N_a\}_{KB}$

Figure 8. The Needham-Schroeder-Lowe Protocol is a secure method for establishing secure data transmission.

In this manner A and B each have securely passed their public keys to the other and also have verified that they were able to decrypt the other's message. For Symmetic key exchange after mutual verification, as described in Steps 1–3 above, there would be a Step 4 in which A sends the B Symmetric Key encrypted with B's public key and a combination of the nonce from A and B. Upon receipt, B would retrieve the symmetric key and forward a reply to A including B's nonce and identity encrypted with the symmetric key as a step 6. Step 7 would be A responding to B with its identity and A's nonce encrypted with the symmetric key. Hence both parties are able to communicate securely using the shared symmetric key.

XML key exchange follows the World Wide Web Consortium (W3C) 2005 XML Key Management Specification recommendation. The following XML code has been generated based upon Bilal Siddiqui's tutorial "Exploring XML Encryption, Part 1 Demonstrating the secure exchange of structured data" article that was posted on IBM's Web site (Siddiqui, 2009).



```
<?xml version="1.0" encoding="UTF-8"?>
<AssymetricKeyExchangeDemonstration>
          <EncryptedKey  CarriedKeyName="John Paul Jones."
          xmlns='http://www.w3.org/2001/04/xmlenc#'>
                    <ds:KeyInfo
xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>

          <ds:KeyValue>0afd65fdf6dfdbbszfds9f1sdT03</ds:KeyValue>
                    </ds:KeyInfo>
```

Figure 9. Step 1 of the XML Key Management Specification (XKMS) implementation is similar to the Needham-Shroeder Lowe protocol in which is an XML Request Message encrypted with recipient public key.

The XML Signature <KeyInfo> element identifies a public key. The XML Key Information Service Specification (X-KISS) defines a protocol for a trust service that resolves public key information contained in XML Signature <KeyInfo> elements. X-KISS supports two service tiers: Locate and Validate.

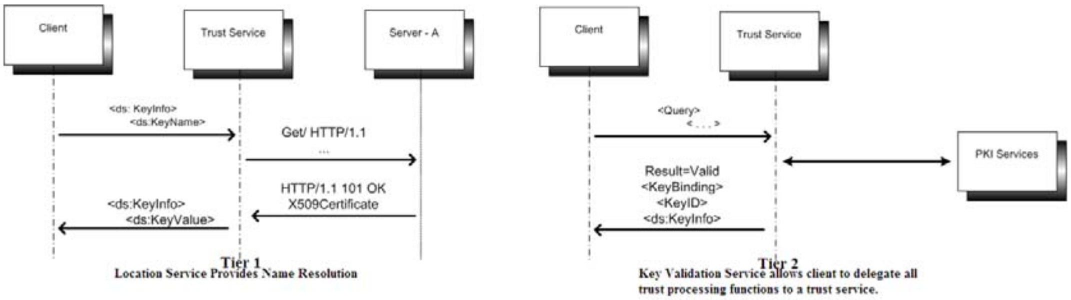


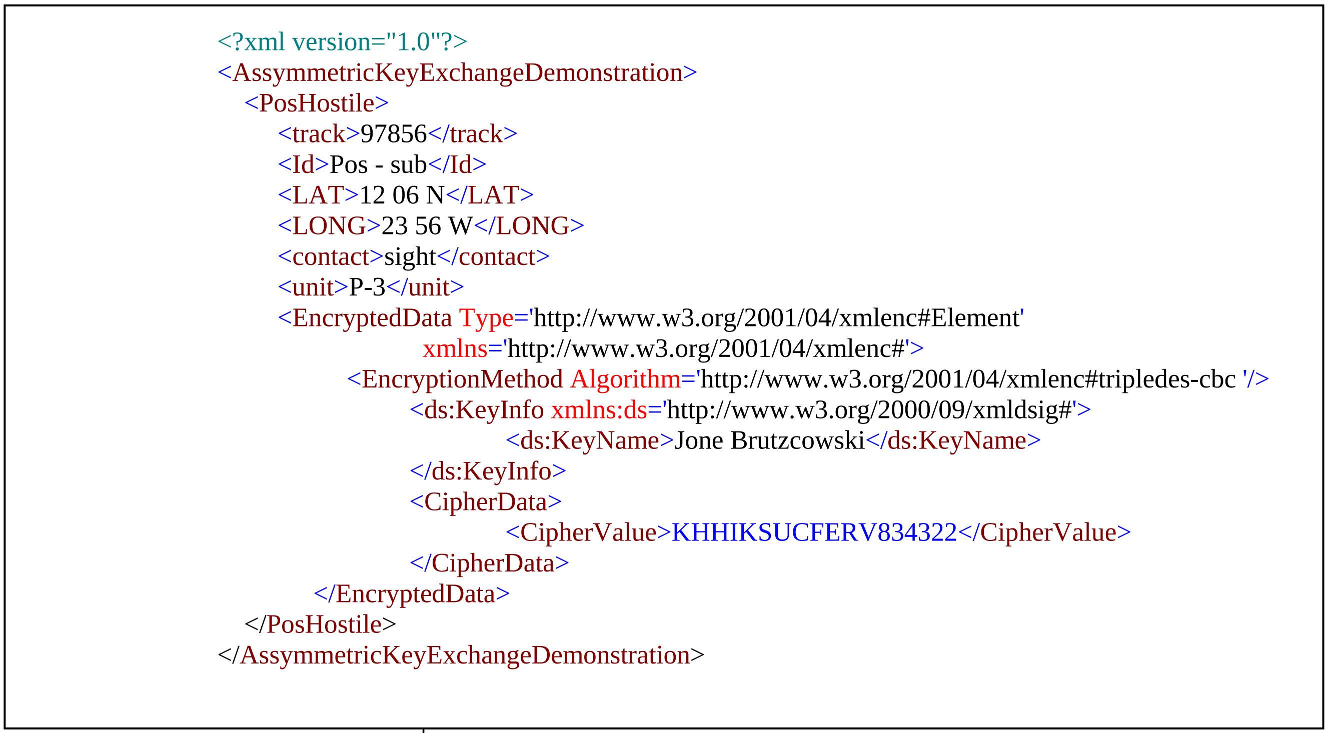
Figure 10. This figure depicts XML Key Information Service Specification (X-KISS) Tier 1 and Tier 2 when used within a public key infrastructure environment (After W3C XKMS Working Group 2009)

The XML Request Message Example—Step 1 displays a message that would be sent containing Jeffrey’s public key. This is a request message as identified in step 1 of the Needham-Schroeder-Lowe protocol defined above.

```
<?xml version="1.0" encoding="UTF-8"?>
<AssymmetricKeyExchangeDemonstration>
        <EncryptedKey CarriedKeyName="Jones Brutzcowski"
         xmlns='http://www.w3.org/2001/04/xmlenc#'>
                <EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                <CipherData>

        <CipherValue>safr3425fdot49sdfsfadfhydbceydf3rfdsgcv</CipherValue>
                </CipherData>
        </EncryptedKey>
</AssymmetricKeyExchangeDemonstration>
```

Figure 11. Responding to the XML request message, the sender returns the message containing the recipients public key encrypted with the senders public key. This is step 2 of the specification entitled the XML Response Message.



```
<?xml version="1.0"?>
<AssymmetricKeyExchangeDemonstration>
  <PosHostile>
     <track>97856</track>
     <Id>Pos - sub</Id>
     <LAT>12 06 N</LAT>
     <LONG>23 56 W</LONG>
     <contact>sight</contact>
     <unit>P-3</unit>
     <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
                  xmlns='http://www.w3.org/2001/04/xmlenc#'>
           <EncryptionMethod Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-cbc '/>
                 <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
                        <ds:KeyName>Jone Brutzcowski</ds:KeyName>
                 </ds:KeyInfo>
                 <CipherData>
                        <CipherValue>KHHIKSUCFERV834322</CipherValue>
                 </CipherData>
        </EncryptedData>
  </PosHostile>
</AssymmetricKeyExchangeDemonstration>
```

Figure 12. In the final 3rd and final step, both parties now know that they can communicate securely with one another and start to exchange data. The above figure utilizes the 3DES cipher block chaining encryption algorithm.

The XML text is the response message in which Brutzcowski supplies a randomly generated secret key encrypted with Williams' public key. This is equivalent of Step 2 of the protocol described above.

Figure 12 is step 3 of the protocol described in Figure 8, which the Jones sends Brutzcowski a message with some data that has been encrypted with Brutzcowski's public key. The aforementioned discussion on key exchange was integrated to present a general idea of what is involved within the process, however, it is beyond the scope of this thesis to discuss in detail and contrast the various methods of key exchange.

Key management is an integral part of the overall process, and it is assumed that the corporation implementing the technology has competent system architects that are capable of deploying systems capable of the various forms of key management that is acceptable within their security policy. In accordance with the specification version 2.0

for XML key exchange, there are no nounces generated in the initial request. It is generated during the response to the initial request as illustrated in Figure 13.

Request 1

```
<?xml version="1.0" encoding="utf-8"?>
<LocateRequest Id="Ia1d6ca7a067fdd545f1a1396d2f26779"
      Service="http://www.example.org/XKMS"
      xmlns="http://www.w3.org/2002/03/xkms#">

<ResponseMechanism>http://www.w3.org/2002/03/xkms#Represent</ResponseMec
hanism>
  <QueryKeyBinding />
</LocateRequest>
```

Response 1

```
<?xml version="1.0" encoding="utf-8"?>
<LocateResult Id="Idbc77142059a3a51c9eccd2425d77757"
      Service="http://www.example.org/XKMS"
      Nonce="Rj2BoUZM7PisPX2ytSAAWA=="
      ResultMajor="http://www.w3.org/2002/03/xkms#Represent"
      RequestId="Ia1d6ca7a067fdd545f1a1396d2f26779"
      xmlns="http://www.w3.org/2002/03/xkms#" />
```

Request 2

```
<?xml version="1.0" encoding="utf-8"?>
<LocateRequest Id="I47804adaec32e34afeecdb51f3e0f765"
      Service="http://www.example.org/XKMS"
      Nonce="Rj2BoUZM7PisPX2ytSAAWA=="
      OriginalRequestId="Ia1d6ca7a067fdd545f1a1396d2f26779"
      xmlns="http://www.w3.org/2002/03/xkms#">
  <QueryKeyBinding />
</LocateRequest>
```

Response 2

```
<?xml version="1.0" encoding="utf-8"?>
<LocateResult Id="I3b0111d2232507a56444c1bc85409a94"
      Service="http://www.example.org/XKMS"
      ResultMajor="http://www.w3.org/2002/03/xkms#Success"
      RequestId="I47804adaec32e34afeecdb51f3e0f765"
      xmlns="http://www.w3.org/2002/03/xkms#" />
```

Figure 13. The W3C XML Key Management Specification 2.0 two-phase key exchange protocol implements the use of nonces which further enhances security (Hallam-Baker et al 2005).

To register, renew, revoke, recover, and provide services for roaming the XML Key Registration Service Specification (X-KRSS) protocol provides a trust service for key information. For further information on XML Key Exchange review the W3C XKMS 2.0 recommendation (XKMS Working Group 2005).

2. Well-formed XML

An XML document can be created from a variety of tools, including simple text editors. However, there are certain requirements that are characteristics to all XML documents. All XML documents must be well-formed at bare minimum. Simply put a well formed document is one that consists of valid XML syntax as defined by the W3C. The base requirements for well-formedness are (XML Core Working Group 2008):

- Documents must have a root element
- Elements must have a closing tag
- Tags are case sensitive
- Elements must be properly nested
- Attribute values must always be quoted

Strict adherence to the standard is required to ensure data is processed correctly by all participants within a hastily formed network with multinational and/or multi-agency participants. Failure to comply may result in rejection of the message by one or more of the participants. Refer to the W3C at http://www.w3.org/TR/xml/#sec-well-formed for additional information on the specific constraints on well formed XML.

A simple example of a well formed document can be generated utilizing the Naval Postgraduate School's 3D Dimensional (X3D) graphics authoring tool X3D-Edit 3.2. An example of a simple set of shapes constructed utilizing the tool follow.

3. XML Validation Against a Schema

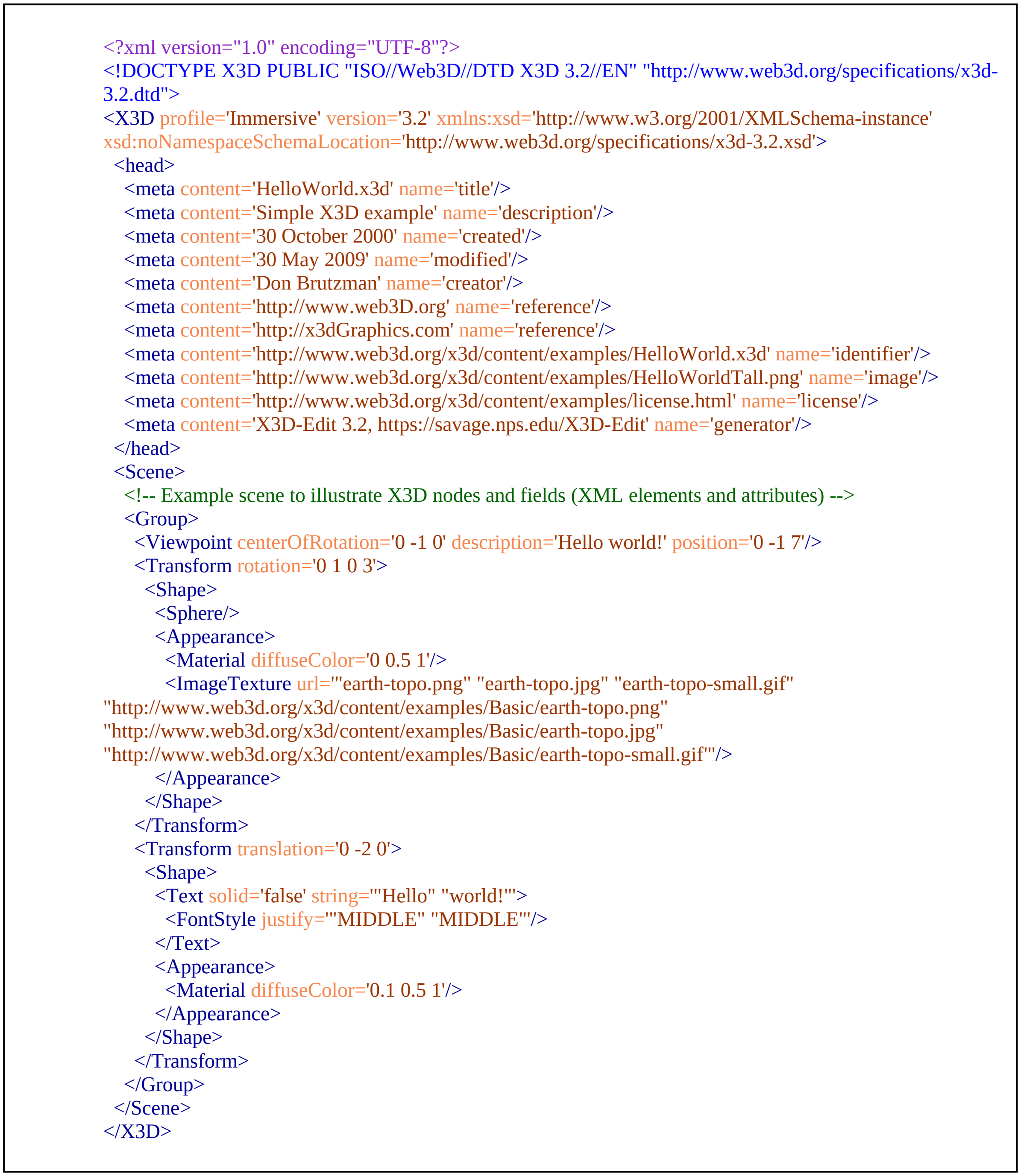
An XML Schema provides a means for defining the structure, content and semantics of XML documents. It expresses shared vocabularies and allows machines to carry out rules made by people (NIST MSID). Schemas are not required for every XML document. However, they simplify tasks if properly integrated within the operational environment. It ensures that data is in the appropriate format to be viewed by all others using the same schema. Alternatively, if another entity views data in a different manner, the schema can be constructed to converted data between an industry specific format and a general base format such that multiple users can exchange information from a common data repository.

4. XML Canonicalization

Canonicalization (C14) is the process of converting data to the simplest and most significant form or schemata to which general equations, statements, or expressions may be reduced without loss of generality. This can be done to compare different representations for equivalence, to count the number of distinct data structures, to improve the efficiency of various algorithms by eliminating repeated calculations, or to make it possible to impose a meaningful sorting order (Rawlings 2004). This thesis uses XML Canonicalization as specified in W3C Canonical XML specification (IETF/W3C XML Signature Working Group 2001). The Canonical form of an XML document is the physical representation of the document produced in which the following list is satisfied:

- The document is encoded in UTF-8
- Line breaks normalized to #xA on input, before parsing
- Attribute values are normalized, as if by a validating processor
- Character and parsed entity references are replaced
- CDATA sections are replaced with their character content
- The XML declaration and document type declaration (DTD) are removed
- Empty elements are converted to start-end tag pairs
- Whitespace outside of the document element and within start and end tags is normalized
- All whitespace in character content is retained (excluding characters removed during line feed normalization)
- Attribute value delimiters are set to quotation marks (double quotes)
- Special characters in attribute values and character content are replaced by character references
- Superfluous namespace declarations are removed from each element
- Default attributes are added to each element
- Lexicographic order is imposed on the namespace declarations and attributes of each element

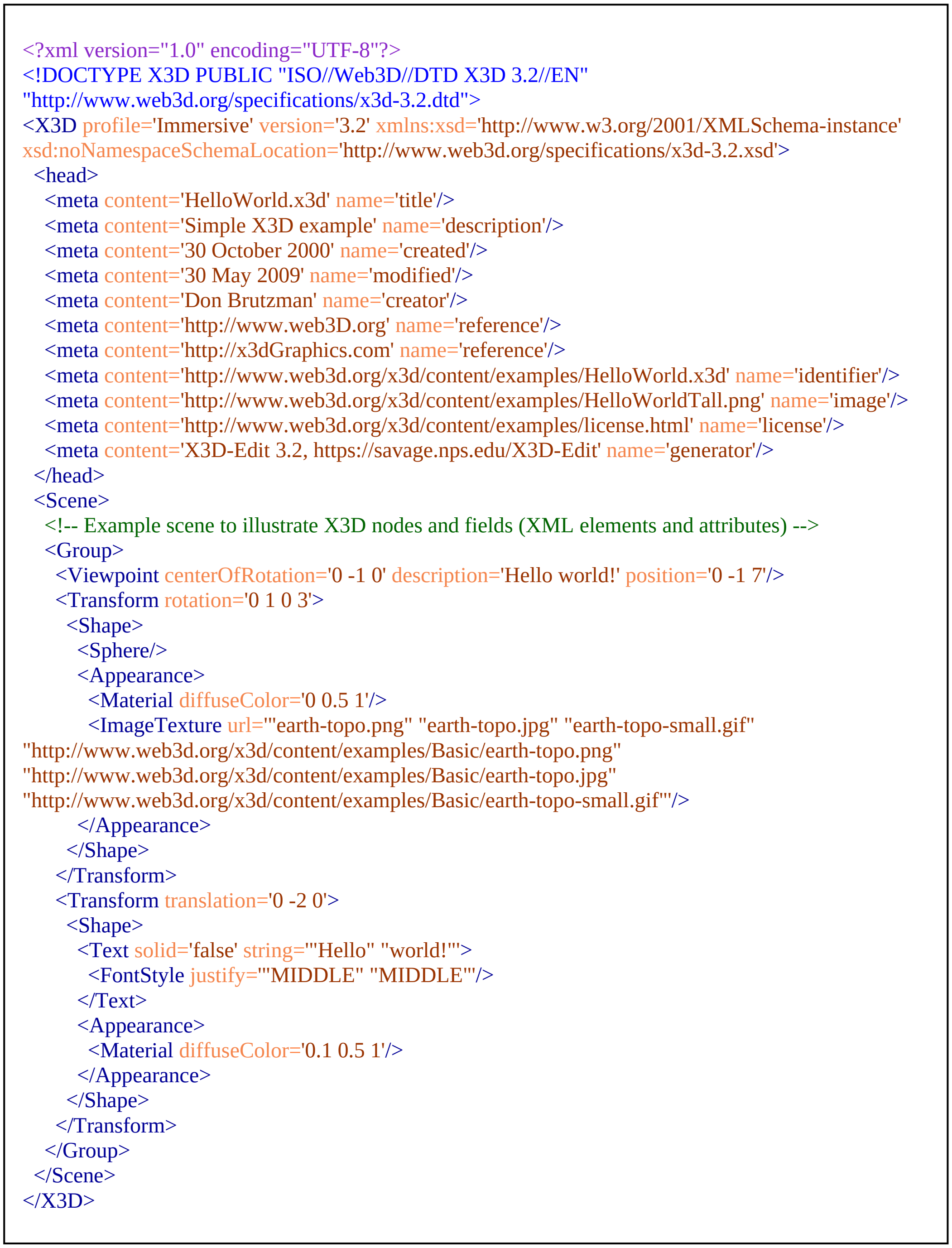
Figures 14 and Figure 15 depict a simple XML document written with X3D-Edit 3.2 before and after C14N has been applied.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.2//EN" "http://www.web3d.org/specifications/x3d-
3.2.dtd">
<X3D profile='Immersive' version='3.2' xmlns:xsd='http://www.w3.org/2001/XMLSchema-instance'
xsd:noNamespaceSchemaLocation='http://www.web3d.org/specifications/x3d-3.2.xsd'>
  <head>
    <meta content='HelloWorld.x3d' name='title'/>
    <meta content='Simple X3D example' name='description'/>
    <meta content='30 October 2000' name='created'/>
    <meta content='30 May 2009' name='modified'/>
    <meta content='Don Brutzman' name='creator'/>
    <meta content='http://www.web3D.org' name='reference'/>
    <meta content='http://x3dGraphics.com' name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/HelloWorld.x3d' name='identifier'/>
    <meta content='http://www.web3d.org/x3d/content/examples/HelloWorldTall.png' name='image'/>
    <meta content='http://www.web3d.org/x3d/content/examples/license.html' name='license'/>
    <meta content='X3D-Edit 3.2, https://savage.nps.edu/X3D-Edit' name='generator'/>
  </head>
  <Scene>
    <!-- Example scene to illustrate X3D nodes and fields (XML elements and attributes) -->
    <Group>
      <Viewpoint centerOfRotation='0 -1 0' description='Hello world!' position='0 -1 7'/>
      <Transform rotation='0 1 0 3'>
        <Shape>
          <Sphere/>
          <Appearance>
            <Material diffuseColor='0 0.5 1'/>
            <ImageTexture url='"earth-topo.png" "earth-topo.jpg" "earth-topo-small.gif"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo.png"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo.jpg"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo-small.gif"'/>
          </Appearance>
        </Shape>
      </Transform>
      <Transform translation='0 -2 0'>
        <Shape>
          <Text solid='false' string='"Hello" "world!"'>
            <FontStyle justify='"MIDDLE" "MIDDLE"'/>
          </Text>
          <Appearance>
            <Material diffuseColor='0.1 0.5 1'/>
          </Appearance>
        </Shape>
      </Transform>
    </Group>
  </Scene>
</X3D>
```

Figure 14. X3D files are XML compliant. However, before the application of Canonicalization (C14N) unnecessary space is consumed.

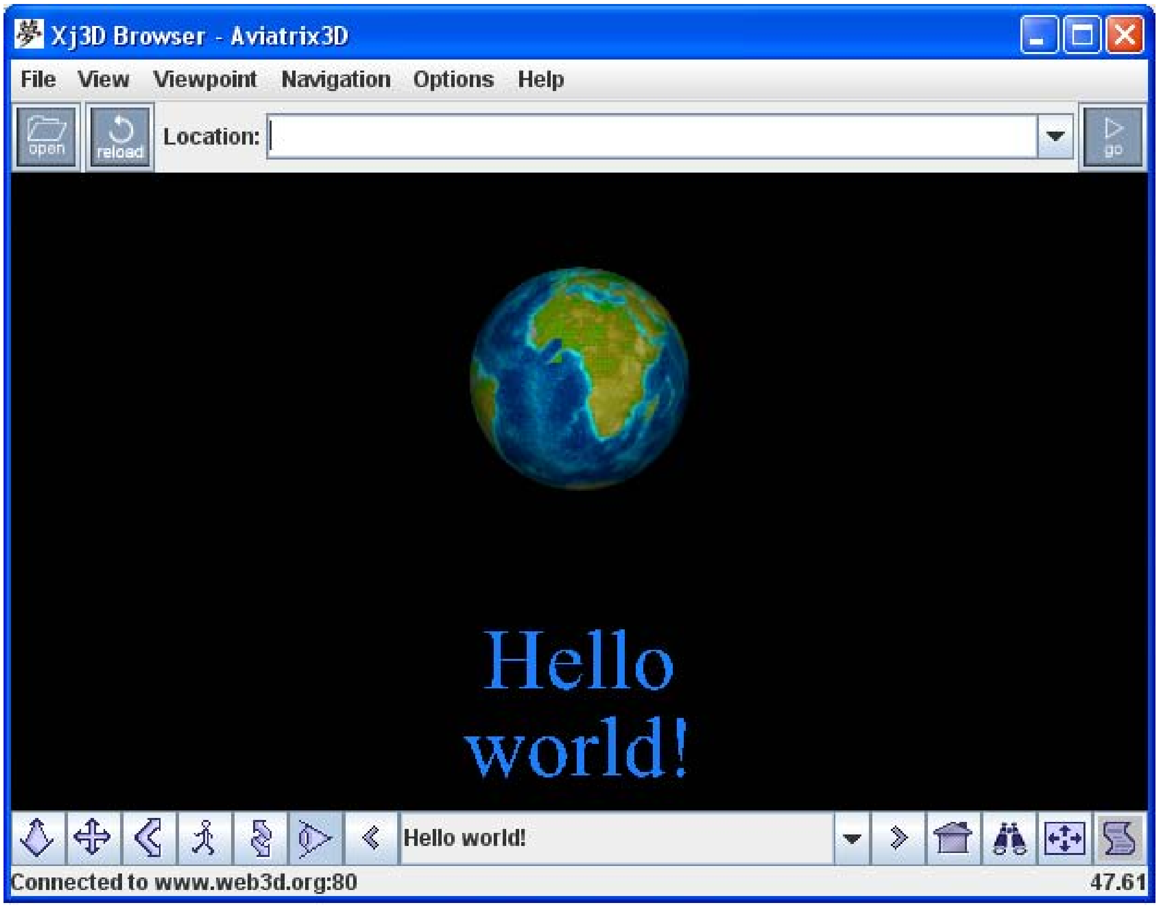
Notice in Figure 14 , there is space which may make the document easier to read for the average human. However, each character makes the file larger. Additionally, in accordance with the W3C XML Signature Syntax and Processing recommendation canonicalization is a prerequisite for creation of a digital signature. All implementations of C14N that are compatible with the specification are allowed with XML Encryption and Authentication. It is helpful for interoperability within a cooperative multinational and multiagency environment whether at sea or ashore that default attribute values be omitted to resolve message size as in the example of X3D C14N. Digital signatures are discussed later in the document. X3D Edit supports both the X3D specification and also the XML specification for Canonicalization throught the X3D-Edit menu option. X3D Edit offers an array of robust security features that are in full compliance with the W3C XML, W3C Digital Signature and Syntax Processing, and W3C XML Encyption Recommendations. It is a graphic and visualization authoring tool that sets the bar for integration of security products within to facilitate code signing and encryption in addition to the ability to process, verify and decrypt encrypted and digitally signed documents. See appendix D for further a further description of X3D edits security capabilities, as it relates to XML Encryption and authentication.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.2//EN"
"http://www.web3d.org/specifications/x3d-3.2.dtd">
<X3D profile='Immersive' version='3.2' xmlns:xsd='http://www.w3.org/2001/XMLSchema-instance'
xsd:noNamespaceSchemaLocation='http://www.web3d.org/specifications/x3d-3.2.xsd'>
  <head>
    <meta content='HelloWorld.x3d' name='title'/>
    <meta content='Simple X3D example' name='description'/>
    <meta content='30 October 2000' name='created'/>
    <meta content='30 May 2009' name='modified'/>
    <meta content='Don Brutzman' name='creator'/>
    <meta content='http://www.web3D.org' name='reference'/>
    <meta content='http://x3dGraphics.com' name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/HelloWorld.x3d' name='identifier'/>
    <meta content='http://www.web3d.org/x3d/content/examples/HelloWorldTall.png' name='image'/>
    <meta content='http://www.web3d.org/x3d/content/examples/license.html' name='license'/>
    <meta content='X3D-Edit 3.2, https://savage.nps.edu/X3D-Edit' name='generator'/>
  </head>
  <Scene>
    <!-- Example scene to illustrate X3D nodes and fields (XML elements and attributes) -->
    <Group>
      <Viewpoint centerOfRotation='0 -1 0' description='Hello world!' position='0 -1 7'/>
      <Transform rotation='0 1 0 3'>
        <Shape>
          <Sphere/>
          <Appearance>
            <Material diffuseColor='0 0.5 1'/>
            <ImageTexture url='"earth-topo.png" "earth-topo.jpg" "earth-topo-small.gif"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo.png"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo.jpg"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo-small.gif"'/>
          </Appearance>
        </Shape>
      </Transform>
      <Transform translation='0 -2 0'>
        <Shape>
          <Text solid='false' string='"Hello" "world!"'>
            <FontStyle justify='"MIDDLE" "MIDDLE"'/>
          </Text>
          <Appearance>
            <Material diffuseColor='0.1 0.5 1'/>
          </Appearance>
        </Shape>
      </Transform>
    </Group>
  </Scene>
</X3D>
```

Figure 15. After C14N the XML document maintains its form and removes unnecessary white space. Compare the previous figure with this one and it becomes evident that it has a smaller file size.

In contrast with the previous figure, all unnecessary space has been removed from the document and now the document has a valid format and is ready for additional operations. When this file is operated upon, it produces a useful representation of the Earth with a welcoming banner, as displayed in Figure 16.



Connected to www.web3d.org:80

Figure 16. X3D Edit Scene displayed within XJ3D Browser

5. XML Digital Signature

XML Digital Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere (IETF/W3C XML Signature Working Group). However, there is a specific order of operations that must be adhered in order for the digital signature to be generated. Figure 17 is an illustration of the order of operations as defined by the W3C.

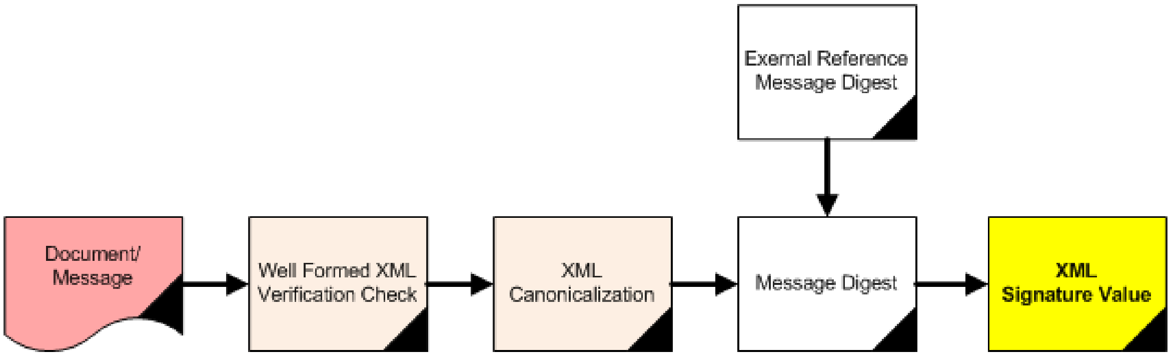


Figure 17. Digital Signature Order of Operations

In order for a document to be a valid XML, it must be well formed. Therefore, it is required to verify that the document is well formed prior to any other operation on it. In accordance with the XML Signature Syntax and Processing specification a document must be well formed, and must have a canonicalization method that is applied prior to being passed through a function to compute the message digests. In computing the message digest, there may also be external references within the document that are also covered by the digital signature. These elements are also used within the computation of the digest. Finally, the digest is used to generate a signature value that by combining the digest and a key dependent algorithm to create the digital signature. Any changes made to the document or external references would invalidate the digital signature. By invalidation the computations generated by the recipient of the XML message would be different than the computation from the original message. For example, let us examine the value of the secure hash and the message digest of the X3D-Edit XML file before and after XML canonicalization by utilizing Linux based tools (md5sum and sha1sum) packaged within CYGWIN and is displayed in Table 1.

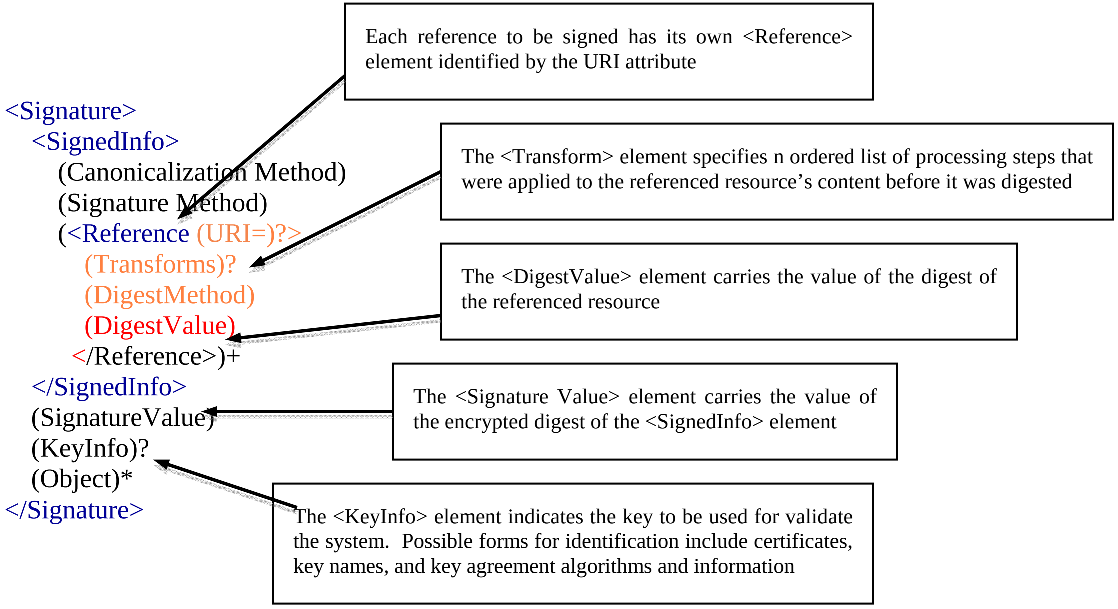
File Name:	C14N-Example
MD5SUM before C14N	120b2fd35f85649bb62a4e17eeb9389d
MD5SUM After C14N	7ce6c6f5b71b46e73b89631421550a87
SHA1SUM Before C14N	c67db0b2427517940ee1f2ce6fa5dc1e7024760c
SHA1SUM After C14N	7c2990813c0adbd16eae86ce54337280e1a85eab

Table 1. Contrast of Canonicalization against X3D-Edit file shows that any alteration to a file changes the integrity hash value of the file even though the content may remain the same.

It is noted from the table above that both the message digest and the secure hash yield different values for the file in it is initial state and its canonicalized form. Based upon this observation, it follows that if a change to the serialized document occurs the signature cannot be verified and thus the file would be rejected from a system, which depends upon the integrity of the file and authenticity of the sender.

6. XML Digital Signature Structure

The XML digital signature follows a specific format as shown in Figure 18:



```
<Signature>
  <SignedInfo>
    (Canonicalization Method)
    (Signature Method)
    (<Reference (URI=)?>
      (Transforms)?
      (DigestMethod)
      (DigestValue)
     </Reference>)+
  </SignedInfo>
  (SignatureValue)
  (KeyInfo)?
  (Object)*
</Signature>
```

Each reference to be signed has its own <Reference> element identified by the URI attribute

The <Transform> element specifies n ordered list of processing steps that were applied to the referenced resource's content before it was digested

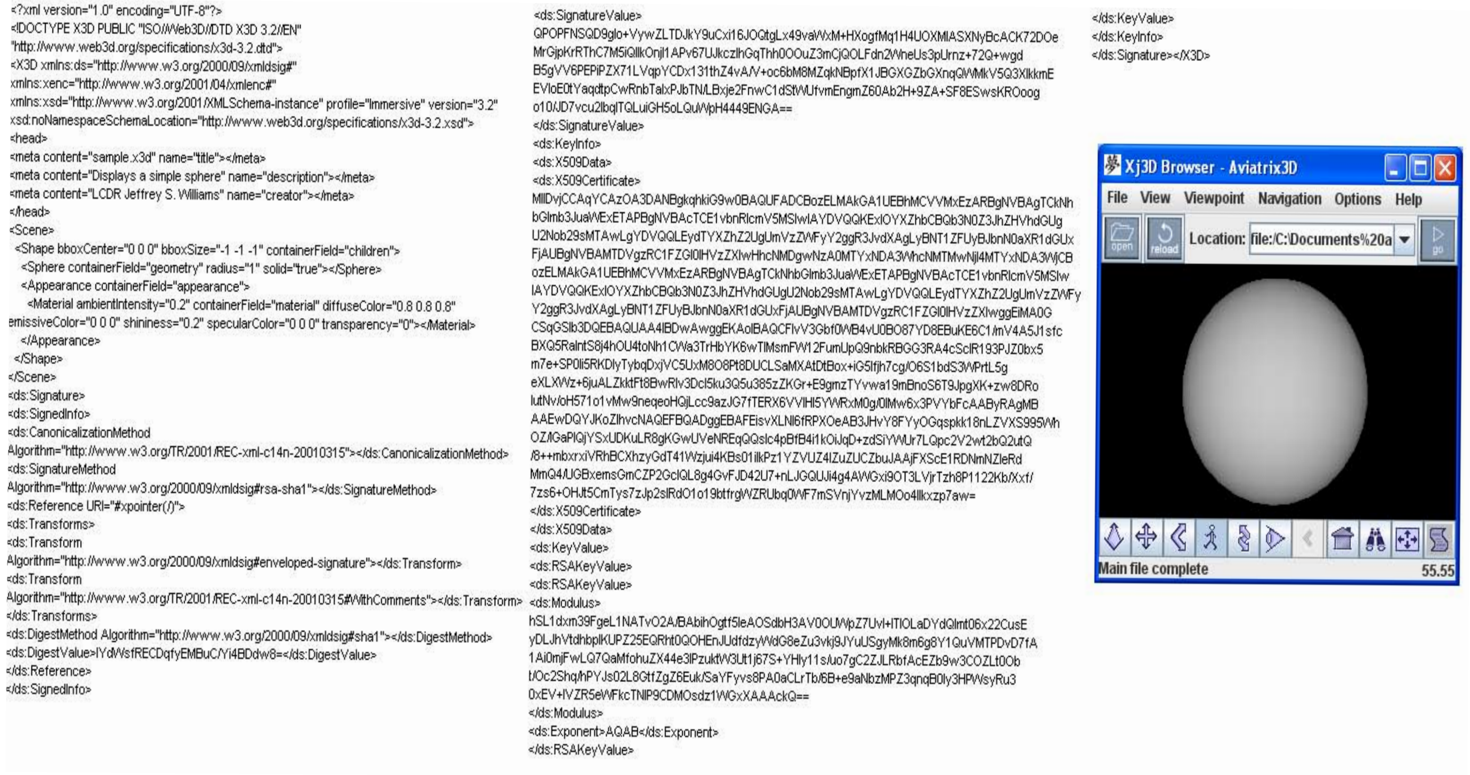
The <DigestValue> element carries the value of the digest of the referenced resource

The <Signature Value> element carries the value of the encrypted digest of the <SignedInfo> element

The <KeyInfo> element indicates the key to be used for validate the system. Possible forms for identification include certificates, key names, and key agreement algorithms and information

Figure 18. The digital signature format contains mandatory and optional parts

Strict adherence to the format is essential to avoid compatibility issues. Examining the figure above, the symbols "?" , "+", and "*" are appear. These symbols have a definite meaning for anyone that is developing or using a uniform translation utility. The "**?**" symbol specifies **zero or one** occurrences. The "*****" indicates **zero or more** occurrences. The "**+**" indicates **one or more** occurrences. Therefore, it is possible to have a digital signature element without a Reference, Transform, Object or KeyInfo tag set. However, for the purposes of this thesis it is assume that all tags are employed and that those that go unused remain empty or converted to a singleton via the C14N process. X3D-Edit 3.2 implementation of digital signature is an excellent working example of it being integrated in an open source application. All that is necessary is to encode a well formed XML document, specify the name space for digital signature and append the digital signature elements at the end of the document as shown in Figure 19, which represents an X3D image of a sphere.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.2//EN"
"http://www.web3d.org/specifications/x3d-3.2.dtd">
<X3D xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance" profile="Immersive" version="3.2"
xsd:noNamespaceSchemaLocation="http://www.web3d.org/specifications/x3d-3.2.xsd">
<head>
<meta content="sample.x3d" name="title"></meta>
<meta content="Displays a simple sphere" name="description"></meta>
<meta content="LCDR Jeffrey S. Williams" name="creator"></meta>
</head>
<Scene>
 <Shape bboxCenter="0 0 0" bboxSize="-1 -1 -1" containerField="children">
  <Sphere containerField="geometry" radius="1" solid="true"></Sphere>
  <Appearance containerField="appearance">
   <Material ambientIntensity="0.2" containerField="material" diffuseColor="0.8 0.8 0.8"
emissiveColor="0 0 0" shininess="0.2" specularColor="0 0 0" transparency="0"></Material>
  </Appearance>
 </Shape>
</Scene>
<ds:Signature>
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
<ds:Reference URI="#xpointer(/)">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
<ds:Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"></ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>lYdWsfRECDqfyEMBuC/Yi4BDdw8=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
QPOPFNSQD9glo+VywZLTDJkY9uCxi16JOQtgLx49vaWxM+HXogfMq1H4UOXMIASXNyBcACK72DOe
MrGjpKrRThC7M5iQllkOnjl1APv67UJkczlhGqThh0OOuZ3mCjQOLFdn2WneUs3pUrnz+72Q+wgd
B5gVV6PEPiPZX71LVqpYCDx131thZ4vA/V+oc6bM8MZqkNBpfX1JBGXGZbGXnqQWMkV5Q3XlkkmE
EVloE0tYaqdtpCwRnbTalxPJbTN/LBxje2FnwC1dStWUfvmEngmZ60Ab2H+9ZA+SF8ESwsKROoog
o10/JD7vcu2lbqITQLuiGH5oLQuWpH4449ENGA==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIDvjCCAqYCAzOA3DANBgkqhkiG9w0BAQUFADCBozELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExETAPBgNVBAcTCE1vbnRlcmV5MSIwIAYDVQQKExlOYXZhbCBQb3N0Z3JhZHVhdGUg
U2Nob29sMTAwLgYDVQQLEydTYXZhZ2UgUmVzZWFyY2ggR3JvdXAgLyBNT1ZFUyBJbnN0aXR1dGUx
FjAUBgNVBAMTDVgzRC1FZGl0IHVzZXIwHhcNMDgwNzA0MTYxNDA3WhcNMTMwNjI4MTYxNDA3WjCB
ozELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCE1vbnRlcmV5MSIw
IAYDVQQKExlOYXZhbCBQb3N0Z3JhZHVhdGUgU2Nob29sMTAwLgYDVQQLEydTYXZhZ2UgUmVzZWFy
Y2ggR3JvdXAgLyBNT1ZFUyBJbnN0aXR1dGUxFjAUBgNVBAMTDVgzRC1FZGl0IHVzZXIwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCFIvV3Gbf0WB4vU0BO87YD8EBuKE6C1/mV4A5J1sfc
BXQ5RaIntS8j4hOU4toNh1CWa3TrHbYK6wTIMsmFW12FumUpQ9nbkRBGG3RA4cScIR193PJZ0bx5
m7e+SP0li5RKDlyTybqDxjVC5UxM8O8Pt8DUCLSaMXAtDtBox+iG5Ifjh7cg/O6S1bdS3WPrtL5g
eXLXWz+6juALZkktFt8BwRIv3Dcl5ku3Q5u385zZKGr+E9gmzTYvwa19mBnoS6T9JpgXK+zw8DRo
lutNv/oH571o1vMw9neqeoHQjLcc9azJG7fTERX6VVIHI5YWRxM0g/0lMw6x3PVYbFcAAByRAgMB
AAEwDQYJKoZIhvcNAQEFBQADggEBAFEisvXLNl6fRPXOeAB3JHvY8FYyOGqspkk18nLZVXS995Wh
OZ/lGaPlQjYSxUDKuLR8gKGwUVeNREqQQsIc4pBfB4i1kOiJqD+zdSiYWUr7LQpc2V2wt2bQ2utQ
/8++mbxrxiVRhBCXhzyGdT41Wzjui4KBs01ilkPz1YZVUZ4IZuZUCZbuJAAjFXScE1RDNmNZIeRd
MmQ4/UGBxemsGmCZP2GclQL8g4GvFJD42U7+nLJGQUJi4g4AWGxi9OT3LVjrTzh8P1122Kb/Xxf/
7zs6+OHJt5CmTys7zJp2sIRdO1o19btfrgWZRUbq0WF7mSVnjYvzMLMOo4llkxzp7aw=
</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
hSL1dxm39FgeL1NATvO2A/BAbihOgtf5leAOSdbH3AV0OUWpZ7Uvl+ITIOLaDYdQlmt06x22CusE
yDLJhVtdhbplKUPZ25EQRht0QOHEnJUdfdzyWdG8eZu3vkj9JYuUSgyMk8m6g8Y1QuVMTPDvD7fA
1Ai0mjFwLQ7QaMfohuZX44e3lPzuktW3Ut1j67S+YHly11s/uo7gC2ZJLRbfAcEZb9w3COZLt0Ob
t/Oc2Shq/hPYJs02L8GtfZgZ6Euk/SaYFyvs8PA0aCLrTb/6B+e9aNbzMPZ3qnqB0ly3HPWsyRu3
0xEV+lVZR5eWFkcTNlP9CDMOsdz1WGxXAAAckQ==
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature></X3D>
```

Figure 19. A digitally signed XML document can be much larger than the initial file as shown in the X3D document that generates a primitive sphere

Figure 19 can be viewed in a host of X3D viewers. It is viewed in the open source application Xj3D Browser that is available via World Wide Web Consortium site at http://www.web3d.org/x3d/content/examples/X3dResources.html#Applications.

D. ENCRYPTION

1. XML Encryption Format

Confidentiality is a key element in attaining the goals ascribed to a secure document. Encryption is the means by which confidentiality is attained. Encryption itself is a mathematical method of scrambling readable data into a non-readable form called cyphertext. XML has a very simple format for establishing encrypted data. Figure 20 describes the base structure:

```
<EncryptedData Id? Type? MimeType? Encoding?>
   <EncryptionMethod/>?
   <ds:KeyInfo>
       <EncryptedKey>?
       <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>?
   <CipherData>
     <CipherValue>?
     <CipherReference URI?>?
   </CipherData>
   <EncryptionProperties>?
 </EncryptedData>
```

Figure 20. Encryption Data Element Structure (Dillaway, Blair et al 2002)

The language and terminology for natural expressions is uniform and the symbols have the same meanings as those previously identified for digital signatures: “?” denotes zero or one occurrence, “+” denotes one or more occurrences, and “*” denotes zero or more occurrences and the empty element tag means the element must be empty (Dillaway 2002). There are a host of reasons why values may be left to include security by obscurity or to hide in plain sight. Security by obscurity may be implemented by making the EncryptionMethod an empty element. This act complicates the job of unauthorized recipients of the document because they must search for other clues as to which algorithm was used to encrypt the document. This may increase the complexity of cracking the code by a sizable amount to the point where the information encrypted becomes stale. Stale information is obsolete and can no longer be used to the advantage of potential attacker. For additional information on XML Encryption formats visit http://www.w3.org/TR/xmlenc-core. Figure 21 represents a encypted X3D-Edit implementation of a primitive sphere that has been encrpted.

```
<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Element"><xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-
cbc"></xenc:EncryptionMethod><xenc:CipherData><xenc:CipherValue>LDjMt0PABvNCdRLYpMRiz7p622
eXxw22Kg9/kwUiLUaOEAytAEAEZanihtSPk2sEmlSYbNUKGoUK
7LnkArmRywcrswd1JWrEybU6oXa9omPJIJqCcWPPnv2dtyCsM7EPzDaL2TnqYLJd93RsW6ykecBm

                    <!—Additional Data omitted -->
```

Figure 21. Encryption changes plaintext to cyphertext such that the original information is not discernable from the encrypted variant. This establishes confidentiality.

Encrypted data files generally exceed the length of the original file. Each character that is viewed in this document is represented as bits of 1s and 0s such that there are $2^{\text{key length}}$ different possibilities for a symmetric key system. Each bit is processed by the encryption algorithm, which utilizes the encryption key. The encryption key may be some very large prime numbers. As each bit is processed by the key, there exists a degree of randomness, commonly referred to as entropy. As the degree of entropy increases, the level of difficulty to break the key follows suite. However, this is not to say that the key key length determines the degree of entropy. The algorithm that is employed also determines the degree of entropy in play. The ASCII equivalent of the file after processing is vastly different than the original. Therefore, a relationship exists between the encryption key length and the resulting file size (Williams).

2. Two Party Cascade Protocol Example

Encryption is a method of secure communications exchange in which parties have a key such that the message can be deciphered and read. There are a number of methods for encrypting data. To simplify the initial discussion, the cascade two party protocol is presented. Given arbitrary users X and Y, desiring to exchange messages in which operations α and β are applied to a message M. We can denote this as shown in the Figure 22.

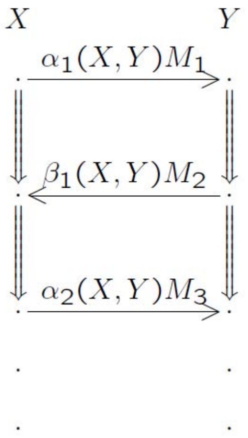


Figure 22. The Dolev Yao Cascade Two Party Protocol is a simple protocol in which the agents α and β can apply several layers of encryption or decryption to the message.

For a transaction to be considered secure utilizing the Dolev Yao cascade two party protocol, the following condtions must be met:

- The intersection of the initial set of operations acted upon alpha with the encyption key of containing the encryption key of X and Y ≠ Ø. For example, if the initial operation was D_xE_x where D is the decryption process and E is an encryption process then it would violate the rule because D_xE_x yields no encryption and therefore, is null. However, $D_xE_xE_y = E_y$ such that the taget is secure meaning encrypted.
- After the initial step for subsequent steps must hold balanced with respect to X. (Bebaïssa 2008)

E. PUBLIC KEY CRYPTOGRAPHY (PKC)

1. Public Key Cryptography (PKC)

Public key cryptography is an asymmetric encryption standard that covers RSA Encryption, Diffie-Hellman key agreement, password-based Encryption, extended-certificate syntax, and certification request syntax, as well as selected attributes (Web and XML Glossary). The W3C recommends public key cryptography as the primary means of achieving confidentiality for web based communications.

2. Public Key Infrastructure (PKI)

Public key infrastructure (PKI) is an asymmetric encryption scheme that involves a key pair (public and private) that is associated with an entity that needs to electronically authenticate its identity, sign or encrypt data. As the name suggest, the public key is published and accessible to all whereas the private key is kept secret and is known only by the message originator. For PKI to function properly, every client must have a PKI plug-in that is configured in such a manner to recognize the location of the local PKI repository as displayed in the following image (Hallam-Baker B).

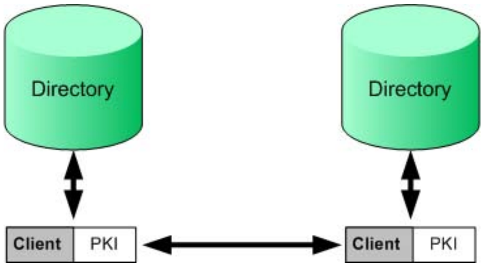


Figure 23. With the traditional PKI model each enclave has its own PKI repository which complicates the maintenance of certificates (After Hallam-Baker, P. et al.)

Implementing an XML Key Management Specification variant of the Traditional PKI utilizing a trust service that interfaces with the underlying PKI achieves a smaller footprint, simpler implementation, centralized configuration of trust relationships, and flexibility to incorporate additional features with neither modifying nor replacing existing clients. Therefore, it essentially makes seamless integration of the technology with the existing architecture as seen in the image below (Hallam-Baker B).

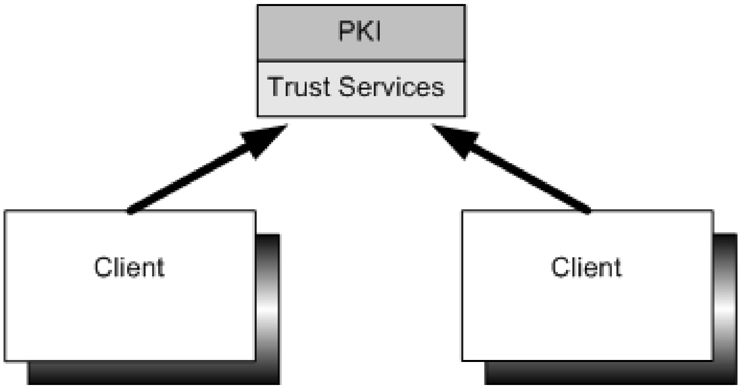


Figure 24. Clients enlist a certificate authority for authorization within the XKMS Trust Services Model (After Hallam-Baker et al).

F. EFFICIENT XML INTERCHANGE (EXI)

1. Compression

EXI is a binary syntax for XML based upon the conclusions of the W3C XML Binary Characterization Working Group (Worthington 2009). Due to the verbose nature of Extensible Markup Language (XML), compression is required to normalize the cost of implementing XML within a bandwidth-constrained environment. As of September 2008, The World Wide Web Consortium (W3C) published a last call working draft for EXI format 1.0 (Efficient XML Interchange Working Group 2008). EXI is a general-purpose format that has shown to work on the entire range of the XML family of languages. Because of its adaptive and flexible nature it achieves compactness results equal to, and normally superior to, alternative compression formats as indicated in the Figure 25 (Sheldon 2009).

Figure 25 is a descriptive illustrative comparison of the performance of various compression compression algorithms in relation to EXI Encryption. It is evident that EXI is the superior lossless compression algorithm in regard to compactness.

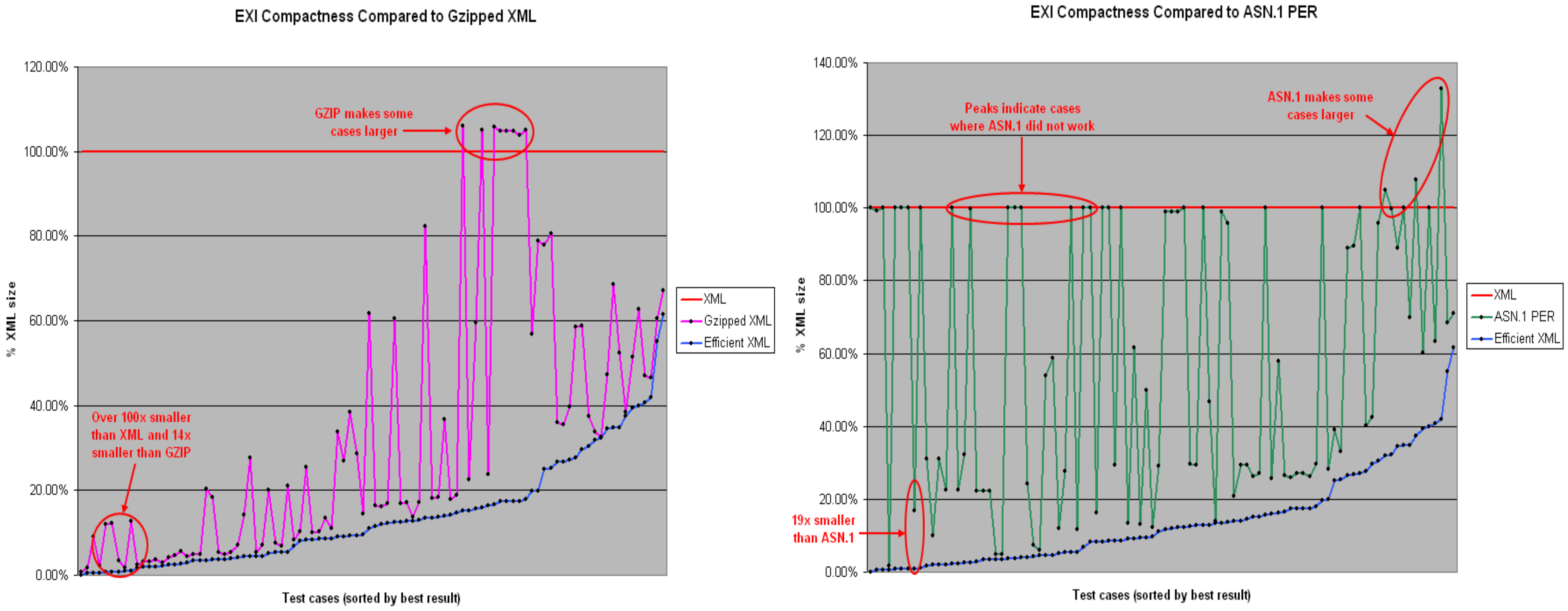


Figure 25. EXI performance comparison with well known compression methods (W3C EXI Working Group 2009)

Table 2 displays results obtained from processing several message files from Appendix A in contrast to GZIP and ZIP compression algorithms. As of this writing, EXI is in final call for the W3C and is on it's way to being a W3C recommendation. The results illustrated in Table 2 are promising.

Input	Technique	Original Size	Technique Size	% of Original
visitRequest.xml	Original	6258	6258	100%
visitRequest.xml	GZipped	6258	1695	27.09%
visitRequest.xml	Zipped	6258	1979	31.62%
visitRequest.xml	**EXI, No Schema**	**6258**	**1084**	**17.32%**
confrencePlanningMSG.xml	Original	19725	19725	100%
confrencePlanningMSG.xml	GZipped	19725	4960	25.15%
confrencePlanningMSG.xml	Zipped	19725	5260	26.67%
confrencePlanningMSG.xml	**EXI, No Schema**	**19725**	**4045**	**20.51%**
EXEMPLAR COMMS PLAN.xml	Original	27793	27793	100%
EXEMPLAR COMMS PLAN.xml	GZipped	27793	5650	20.33%
EXEMPLAR COMMS PLAN.xml	Zipped	27793	5948	21.40%
EXEMPLAR COMMS PLAN.xml	**EXI, No Schema**	**27793**	**5098**	**18.34%**
farewellMSG.xml	Original	3349	3349	100%
farewellMSG.xml	GZipped	3349	1336	39.89%
farewellMSG.xml	Zipped	3349	1618	48.31%
farewellMSG.xml	**EXI, No Schema**	**3349**	**795**	**23.74%**

Table 2. Table 1 displays test results of various methods of compression using EXI.

Visit the World Wide Web Consortium's Web site at http://www.w3.org/XML/EXI for additional information on EXI compression. To date EXI compression algorithms are worthy of supporting secure business transaction and are compatible with XML compliant encryption algorithms.

G. SUMMARY

The effective use of XML key management, digital signature, compression and encryption effectively illustrates a valid secure user-centric interface that seamlessly integrates the security to provide message integrity, authentication, non-repudiation, and confidentiality. These are the four major tenants of network security. The order of operations is of grave concern because if performed in the wrong order the integrity of the message would be in question as the message may be equivalent but not matching the original message due to something as simple as space removal. This leads us to conclude that C14N must be performed prior to generating the digital signature for either the overall message or a fragment thereof. The remaining steps assume that the message has been canonicalized and ready for processing through the remaining steps.

IV. PROBLEM DEFINITION: MULTI-AGENCY/MULTINATIONAL OPERATIONAL DATA SHARING

A. INTRODUCTION

In order to secure the sea lines of communications within a global scope, it is essential to have a means to securely and efficiently exchange information between international entities. Due to the nature of XML as relayed in the XML in 10 points (Chapter III), it is a viable candidate ready for international adoption. However, as with any security implementation, does message and document-centric XML Security address the intended task of facilitating secure dynamic data exchange between partners? XML security is a lightweight security mechanism that when followed in strict accordance with the W3C working group specifications provides an interoperable, efficient means of exchanging data with minimum risks to the existing network architecture. Each process within XML security requirements satisfies a specific function to achieve sender authenticity, message integrity, and confidentiality such that the incorporation of XML security at the document and message level mitigates risk to the corporate network while providing adequate security from secure endpoint to a secure endpoint with minimal exposure to either the sender’s or the receiver’s network architecture.

B. PROBLEM OVERVIEW

Different agencies and different nations are not able to securely communicate and share structured information with each other. The reasons for this are that the information is stored in different data formats and each organization may have a security policy different from that of another agency. The current evolution of data and security policies by different agencies and nations do not resolve this issue. The solution must allow for a diverse communications framework to securely enable shared/common data exchange between traditional and non-traditional actors. Additionally, a mechanism must exist to provide the minimal exchange of cryptographic technology, which can be achieved by implementing open standards technology. The reasons for this are quite simple:

- No nation trusts another nation’s security software
- Innate trust of World Wide Web security because multiple independent implementations are available
- Requirement for a substitute alternative cryptographic algorithm.

Within the scope of a more secure infrastructure, there must be a shift from persistent access to security embedded at the document level. Within this scope document-centric security can be achieved.

The March 2009 issue of Proceedings interviewed 37 international naval commanders-in-chiefs and inquired what they perceived to be the most significant maritime security threat facing their respective nation. 70% of the authors mentioned maintaining the sea lines of communications and 51% mentioned piracy as depicted in Figure 26.

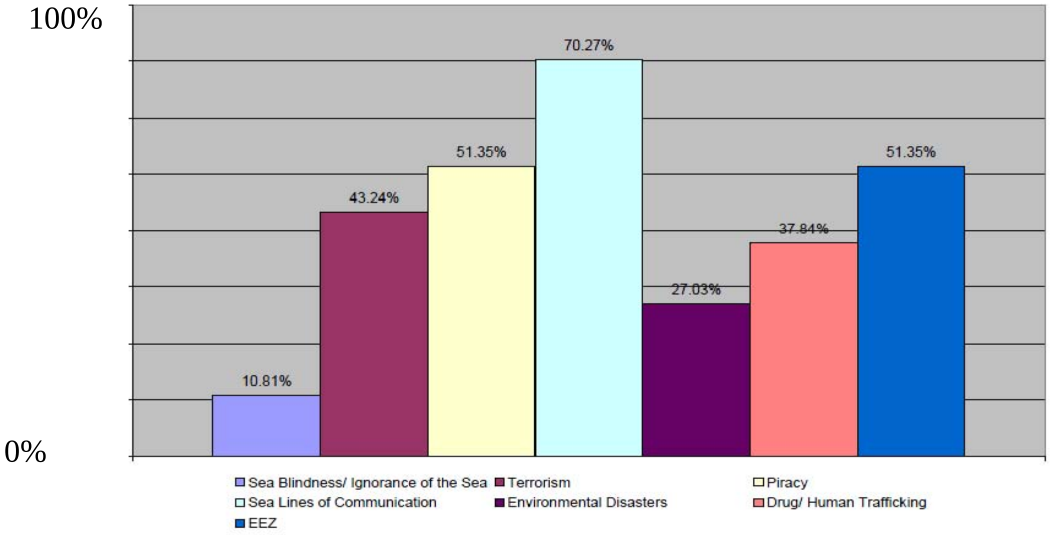
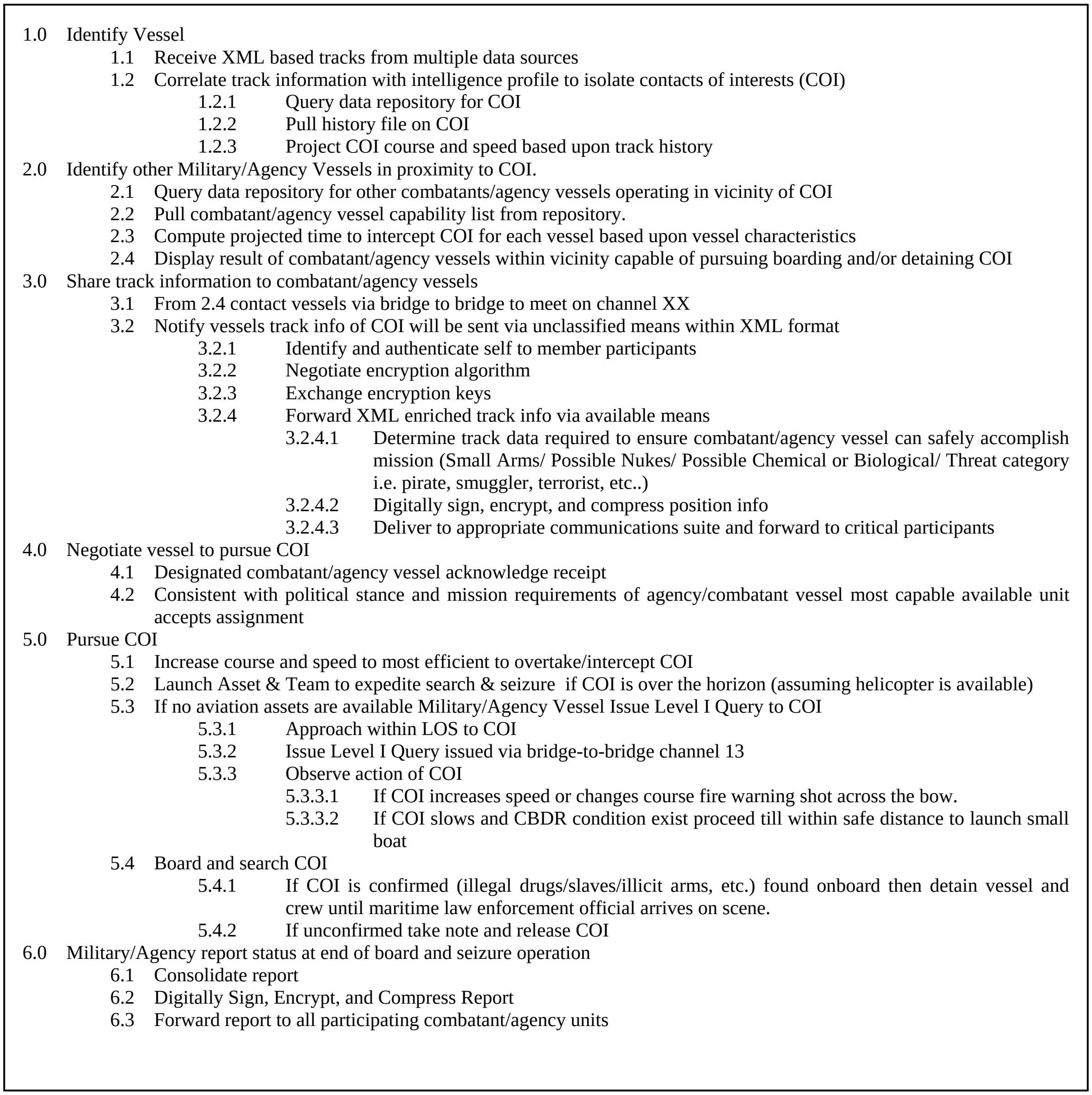


Figure 26. This chart depicts the national concerns of 37 international commanders in respect to their nation’s interests. It is viewed as their nation’s most significant maritime threat. See appendix D for data set constructed from Preceedings March 2009 article.

In order to support the operational objectives of Anti-piracy, Counter Drugs/Human Trafficking, and Anti-terrorist operations, jointly with coalition partners, there exists a requirement to improve upon existing architecture to provide a secure enriched environment capable of passing data dynamicly to members joining and/or augmenting the surface action group. Bridge-to-bridge is a valuable tool but the only record that exists is what is written in the log. By using voice-to-text tools, it is possible to provide support bridge to bridge in concert with maintaining a virtual log of all communications that have transpired. Data communications can also be passed securely from one entity to another using the XML encryption and authentication.

1. XML Encryption and Authentication—Is it Task Appropriate?

The first issue that must be addressed is not whether XML Encryption and Authentication can secure all communications, but is it the right tool to employ to perform an exchange of data between traditional and non-traditional partners in which formal diplomatic agreements may not exist? The answer to this query can only be discerned by performing a task analysis and marrying it to the standing organization's security policy such that the operational commander can be well informed on his decision to deliver pertinent content to a foreign entity in support of national interests. The following is a pseudo-task analysis generated for a notional situation in which each partner nation X are in a position to assist in the pursuit, search and seizure, of a possible narcotics or human trafficking smuggler vessel.



- 1.0 Identify Vessel
  - 1.1 Receive XML based tracks from multiple data sources
  - 1.2 Correlate track information with intelligence profile to isolate contacts of interests (COI)
    - 1.2.1 Query data repository for COI
    - 1.2.2 Pull history file on COI
    - 1.2.3 Project COI course and speed based upon track history
- 2.0 Identify other Military/Agency Vessels in proximity to COI.
  - 2.1 Query data repository for other combatants/agency vessels operating in vicinity of COI
  - 2.2 Pull combatant/agency vessel capability list from repository.
  - 2.3 Compute projected time to intercept COI for each vessel based upon vessel characteristics
  - 2.4 Display result of combatant/agency vessels within vicinity capable of pursuing boarding and/or detaining COI
- 3.0 Share track information to combatant/agency vessels
  - 3.1 From 2.4 contact vessels via bridge to bridge to meet on channel XX
  - 3.2 Notify vessels track info of COI will be sent via unclassified means within XML format
    - 3.2.1 Identify and authenticate self to member participants
    - 3.2.2 Negotiate encryption algorithm
    - 3.2.3 Exchange encryption keys
    - 3.2.4 Forward XML enriched track info via available means
      - 3.2.4.1 Determine track data required to ensure combatant/agency vessel can safely accomplish mission (Small Arms/ Possible Nukes/ Possible Chemical or Biological/ Threat category i.e. pirate, smuggler, terrorist, etc..)
      - 3.2.4.2 Digitally sign, encrypt, and compress position info
      - 3.2.4.3 Deliver to appropriate communications suite and forward to critical participants
- 4.0 Negotiate vessel to pursue COI
  - 4.1 Designated combatant/agency vessel acknowledge receipt
  - 4.2 Consistent with political stance and mission requirements of agency/combatant vessel most capable available unit accepts assignment
- 5.0 Pursue COI
  - 5.1 Increase course and speed to most efficient to overtake/intercept COI
  - 5.2 Launch Asset & Team to expedite search & seizure if COI is over the horizon (assuming helicopter is available)
  - 5.3 If no aviation assets are available Military/Agency Vessel Issue Level I Query to COI
    - 5.3.1 Approach within LOS to COI
    - 5.3.2 Issue Level I Query issued via bridge-to-bridge channel 13
    - 5.3.3 Observe action of COI
      - 5.3.3.1 If COI increases speed or changes course fire warning shot across the bow.
      - 5.3.3.2 If COI slows and CBDR condition exist proceed till within safe distance to launch small boat
  - 5.4 Board and search COI
    - 5.4.1 If COI is confirmed (illegal drugs/slaves/illicit arms, etc.) found onboard then detain vessel and crew until maritime law enforcement official arrives on scene.
    - 5.4.2 If unconfirmed take note and release COI
- 6.0 Military/Agency report status at end of board and seizure operation
  - 6.1 Consolidate report
  - 6.2 Digitally Sign, Encrypt, and Compress Report
  - 6.3 Forward report to all participating combatant/agency units

Figure 27. The task analysis represent the flow of knowledge that evokes a specific response from decision makers in pursuit of a possible contact of interest.

Pre-planned responses originate with a task analysis. Figure 27 is a task analysis for pursuit of a vessel suspected of malicious activities.

As seen in Figure 27, the pursuit requires a substantial amount of automated XML processing in the retrieval, interim calculations, and display of queried information based upon request initiated by the operator. The source and techniques employed to query the information from the SQL data store is beyond the scope of this thesis. Therefore, based upon the displayed pursuit task analysis focus on item 3, 4 and 6, all of which employ the use of XML digital signature, encryption and authentication elements.

Probable cause is an important attribute to the pursuit and must be included in the transmission especially if the closest participating unit is a coalition partner. Under title 14 U.S. Code article 89a, the U.S. coast guard may make inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the United States has jurisdiction, for the prevention, detection, and suppression of violations of laws of the United States (USC Title 14). The reason this law is in scope of the task analysis is that it establishes precedent for the U.S. to pursue the vessel. Other nations may have such laws on the books that grant their maritime force the legal ability to pursue, detain, search, and seize vessels involved in criminal activity as well. The collection and chain of custody of this information is essential to properly prosecution of the suspected vessel after the operation has come to conclusion. The XML messages properly time stamped and holding a persistent XML signature to verify the originator is designed to verify and validate the information for any interval after the event occurred. Therefore, there are information assurance is vital beyond the systems on which the document was created. It must also be a factor from transmission through reception.

2. Information Assurance (IA) Requirements

Information assurance are measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. In view of information assurance requirements with regards to protection of information the commander has to make a decision within moments as critical aspects of the data collected that is required to make a pursuit. The political and mission objectives of the actors involved may be quite different from those of the commander's unit. Nevertheless, a common interest exists under UNCLOS for piracy or regional agreement that supports the cooperation to ensure the sea lines of communications. Therefore, there exists a need to develop a trust relationship for the flow of communications beyond the standard bridge-to-bridge that also minimizes risk to the network or data. Applying XML

Encryption and Authentication at the document level can help based upon the information assurance requirements. The general questions that are of interest to information assurance specialist are in line with the four basic aspects of security (Berners-Lee 1999):

1. Authenticity–Can structured information be delivered to designated parties over an untrusted network?
2. Confidentiality–Is the actual originator of the file an authorized participant?
3. Message Integrity - Has the file been tampered with or altered during transmission?
4. Non-Repudiation–Can the sender later refute that his/her organization sent the information?

For the purpose of this thesis, it is assumed that participating parties bear no malicious intentions towards each other and that their systems are free of malware. Therefore, the analysis of whether XML encryption is the appropriate tool for the task is based on items 1–4.

a. Can Content Rich Data be Delivered to Designated Parties over an Untrusted Network?

An untrusted network is a network that is external to the networks belonging to an organization and which is out of the organization's ability to control or manage (PCI Security Standards Council 2008). The internet is such a creature. Although an organization can put up firewalls, establish demilitarized zones, enable MAC filter, etc., once information leaves the organization's network, it is out of the control of the organization's control. Therefore, if either the internet or direct point to point RF technology is employed there exists the possibility of signals exploitation by unknown entities or an adversary. To guard against exploitation, the life of the data being passed over the network needs to be assessed to properly conduct the risk assessment to national security. Base track data generally has a brief valid lifespan. As long as the principle of need-to-know, the minimal set of information given to accomplish a given task, is strictly adhered, the threat is minimal. For example, to pursue the COI requires at a minimum base course, speed, associated track number, vessel classification, and justification for pursuit to satisfy international political requirements.

The greater the details embedded within the body of information, the more likely the elevation of the level of classification of the information passed. In the example of the task analysis of the pursuit, XML-based data was encrypted to ensure that if compromised in transit, the information would be stale before the discovery of decryption keys by the infiltrator. Therefore, only authorized parties would be able to decrypt and act on the data contained.

In the field of information assurance in relation to cryptography, it is not a matter of if the system can be broken, it is a matter of how long it takes and the number of resources required to break the encryption. For this reason, it is crucial to evaluate the cryptographic algorithms for their inherent characteristics in relation to the data it shall protect. In a well-designed algorithm the larger the key the longer it takes to break via a brute force attack. With document and Message centric security, we aren't concerned with the document being intercepted although precautions are normally taken to discourage the act. If the document were intercepted and XML document-centric security is used, the data contained is preserved. If the data is encrypted, confidentiality is retained for a finite period of time.

b. Is the Originator of the File an Authorized Participant?

The initial step in phase 3 of the pursuit task analysis is the mutual authentication of all actors involved in the pursuit. This can be done in a myriad of ways during the key exchange process. For example, consider the Needham-Shroeder-Lowe protocol in which all participants have access to each other's public key. Let A and B be separate entities that have access to a common trust service (certificate authority) from which they can confirm each other's public key. Therefore, each actor needs only verify his or her identity by sending a randomly generated (value known as a nounce) to the recipient. The nounce (N) is known only to the originator and can only be decrypted by the authorized actor with the corresponding private key. Entity B sends (→) a request to entity A that he wants to communicate with her. Enclosed within his request is his nounce and his identity encrypted with his public key (KB). A responds back to B with his own nounce B's nounce and its own identity all encrypted with A's public key. B decrypts the message and sees A's nounce. B now knows that he can talk with A and that it is indeed A. Now B needs to send back a message to A to let A know that he can indeed communicate, which is done on step 3 of Figure 28, and it illustrates the protocol. It is discussed in greater detail as it relates to XML key management specification (XKMS) in later sections of this thesis.

Step 1. $B \rightarrow A: \{N_b, B\}_{KB}$

Step 2. $A \rightarrow B: \{N_b, N_a, A\}_{KA}$

Step 3. $B \rightarrow A: \{N_a\}_{KB}$

Figure 28. The Needham-Schroeder Lowe Public Key Encryption Protocol is an example of how information is exchanged within an environment implementing public key infrastructure (After Dinolt 2009).

After step 3 of the protocol, the actors know that they can securely communicate with one another and are free to transmit and receive sensitive unclassified information. If PKI is used the identity of the sender is confirmed.

However, let us assume that the network was hastily formed and a key is based upon a shared secret. Whether using a one-time-pad in which plaintext is combined with a secret random used only once or other cryptographic algorithm, the secret key is disseminated to each participant. Since the key is a shared secret, a digital signature element is required to facilitate authentication otherwise, the participants would not be able to identify themselves to one another. A key slogan of Dr. Don Brutzman that he states frequently to his students is "… you get what you inspect not what you expect..." Making no assumptions about the transmission medium the situation may be as illustrated in Figure 29.

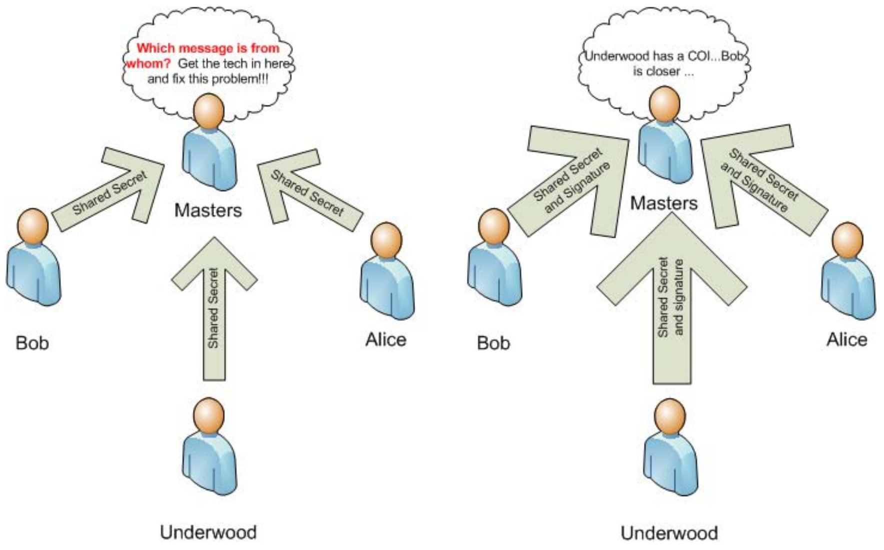

Which message is from whom? Get the tech in here and fix this problem!!!
Masters
Shared Secret
Shared Secret
Shared Secret
Bob
Alice
Underwood
Underwood has a COI...Bob is closer ...
Masters
Shared Secret and Signature
Shared Secret and Signature
Shared Secret and signature
Bob
Alice
Underwood

Figure 29. Digital signature clearly identify and distinguish entities from one another as well as provide a means to support non-repudiation.

In Figure 29, Master receives all messages over an unspecified medium. However, as opposed to trusting the message header information, he's looking for proof of the sender's identity prior to making a decision to release resources or issue directives. On the right side, the Masters receives the messages from all parties and now certain of their identity, is ready to allocate resources to pursue the contact of interest.

c. Message Integrity—Is this the Same as the Original Message

Another information assurance concern with the data is whether or not it had be altered prior to being received. Was the message a victim of the infamous man-in-the-middle attack. The man-in-the-middle attack occurs when the message is intercepted by a third party and during transmission the third party masquerades acts as an intermediary between party A and party B while recording the information. While party A believes that he is coversing with party B, he is communicating with party C and party C forwards messages to party B. Therefore, party A and party B both unwittingly have created secret keys with party C but believe that they are communicating securely with each other. Therefore, if coordinated effectively, transmissions between party A to party B via party C are in accordance with the W3C recommendation for XML encryption. Unknown to parties A and B, party C takes the messages transmitted and repackages them with its own signature. Once the document arrives at its intended recipient, the hash is recomputed and compared with the original message. If it matches, then no compromise occurred; else, reject the message, as it cannot be trusted.   Below is the typical flow chart of the generation of a digitally signed XML document. Therefore, XML innately provides an avenue to validate message integrity with a high assurance of confidence.

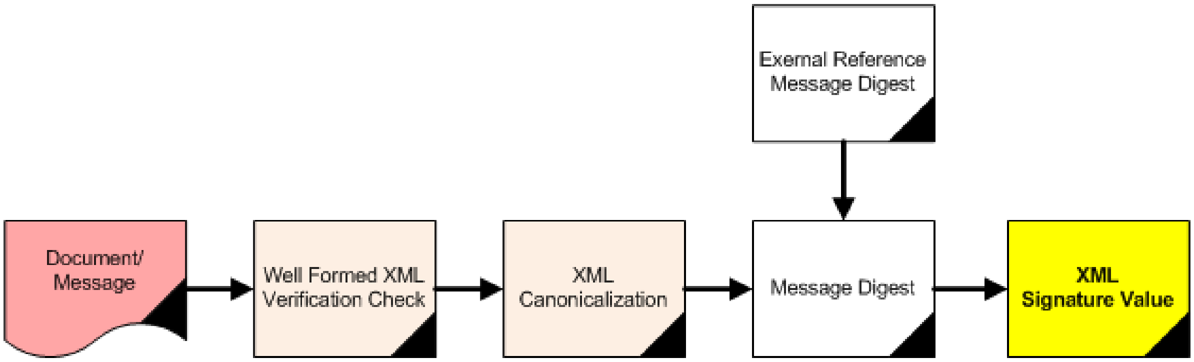


Figure 30. XML Digital signature specification requires that a message be well formed and validated prior to XML Canonicalization. The Canonicalization precedes the generation of the Message Digest . The digest does not only include the XML document but also the digest of any other document or link to which the document refers. After a digest is generated the XML Signature is computed using the digest and the senders private key.

d. Non-repudiation—Can the Sender Later Refute Having Sent the Message?

Non-repudiation is accomplished by means of identity management and audit tracking. It is assumed that the sender is the only entity that has access to his/her digital signature. Therefore, if both the digest and the digital signature are valid then it follows that the message was sent from said individual. “The digital signature utilizing the public and private key must be recognized and not-repudiated (Hwang 2004).”

If authenticity, confidentiality, document integrity and non-reputability are resolved, does XML encryption and authentication applied at the document level provide sufficient information assurance support to satisfy the stringent requirements to make it a general purpose tool? This is an interesting question; however, the answer lies in the strength of the cryptographic algorithm used when sending the message. Once the content is encrypted, it is in a non-intelligible form it reaches a entity with the appropriate corresponding key. However, once the document arrives at its destination and is decrypted security rests solely with the systems security configuration and protections. XML encryption and authentication cannot protect an organization from malicious code nor can it protect it from intrusions. However, it can be used to safely transmit the document from a point A to point B. An encrypted XML document can be transported via a secure sockets layer, which further minimizes the potential hostile exposure to the document. However, for any authentication to work there must exist a level of trust between parties such that the originally distributed keys are trusted and verifiable. Document-centric XML encryption and authentication takes advantage of this trust by ensuring that the discretionary access controls constraints placed upon the file remain valid throughout transmission until the file is decrypted and opened. As such it is not an all-encompassing security mechanism, but it can serve the purpose of transmitting unclassified information among diverse partners over insecure networks in support of combined operations.

C. INTEROPERABILITY AND COMPATIBILITY

Secure exchange of data amongst national and international entities with minimal exchange of hardware and software is required to support dynamic secure communications with traditional and non-traditional partners. However, standing organizations have years of experience with one or more systems of document organization. Tim Berners-Lee wrote "… the key would be to emphasize that it would let each person (organization) retain his own organizational style and software on his computer…" (Berners-Lee 1999) This was stated in during the evolution of what is known today as the World Wide Web. The statement is suitable and continues to hold true today especially when coordinating tasks with multinational and multiagency organizations. The employment of Extensible Stylesheet Language Transformation (XSLT) resolves this to a trivial matter. "XSLT is a declarative programming language, written in XML, for converting XML to some other output without changing the original document." (Hunter 2007 p. 287)

The purpose of an extensible stylesheet transformation (XSLT) is to convert a data file from one format to another without altering the host file. XSLT ranges in complexity from the very simple to computationally complex. A simple method would be to simply declare the fields that are of interest that is desired for the output file such that the output file contains only the desired information.

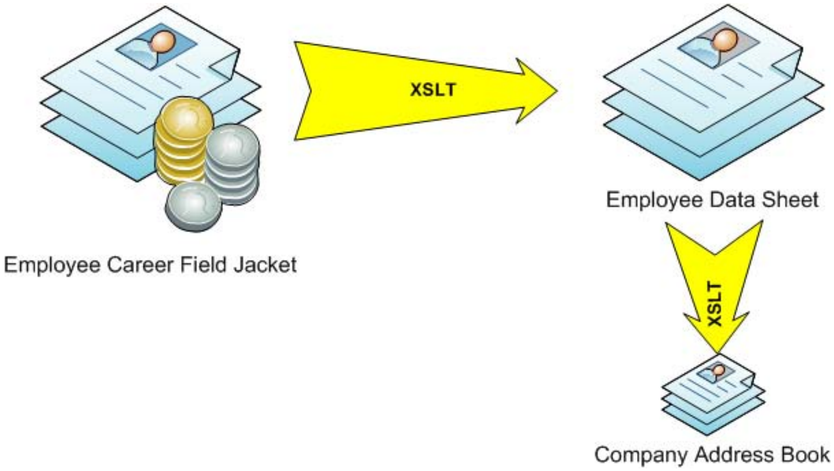
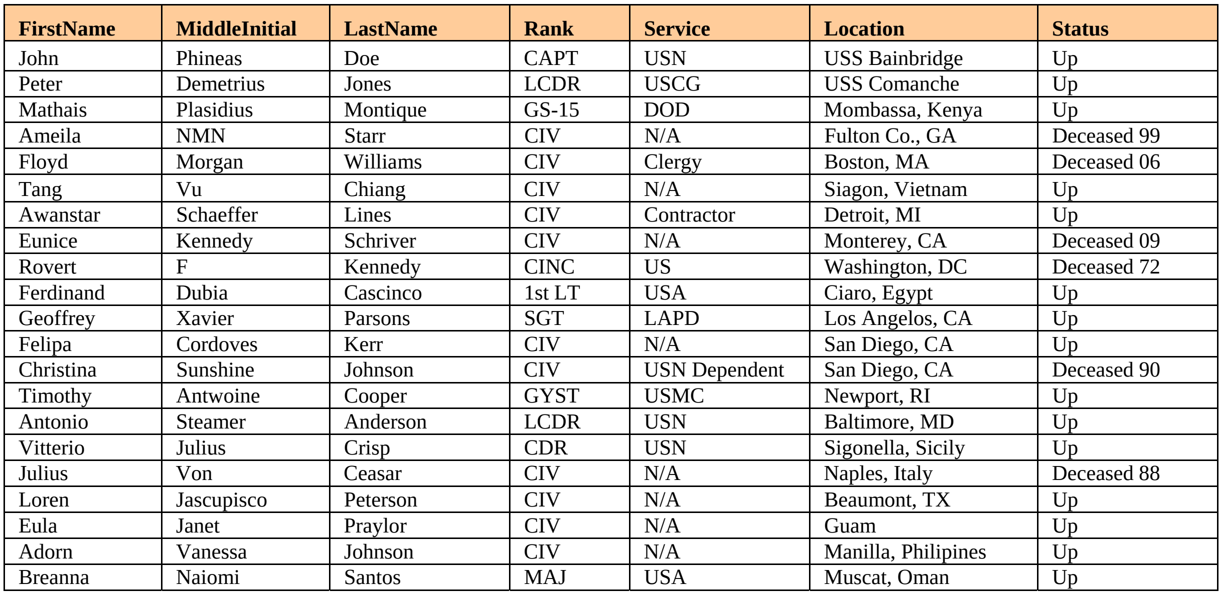


Figure 31. The extensible stylesheet (XSLT) can have a very detailed source and extract only that data which needs be available for a particular group or organization. There is no limit to the number of XSLT employed on a processed dataset.

Adding complexity, as in Figure 31, a robust array of data containing personal identifiable information (PII) and as well as financial records, home and office address can be extracted and parsed using the XSLT to produce subsets of the original files. The XSLT can be used to assist in enforcing organization security policies thereby supporting either a Role Based Access Control (RBAC) in which access to data is restricted only to those that are within certain groups to certain subset of data or using Mandatory Access Control (MAC) in which privileges are even further restricted and generally unyielding. Implementing a Discretionary Access Control (DAC) system, it is possible to rapidly forward data to other organizations. However, caution must be employed whenever the use of DAC is employed, since once information is released the originator no longer has control of the data. Using DAC, the recipient now has full control of the data. By implementing message and document centric security, which protects the data in transit from one endpoint to another endpoint, security can be further embedded to document such that only those individuals with appropriate credentials can have read access. However, it is beyond the scope of this document to investigate document and message centric security on the system once the document arrives on the system.

By isolating the data via an XSLT a very complex system can be made into very simple datasets that contain no PII. There is no limit to the number of times that data can be processed via XSLTs. This means that an XSLT output file can be used as an XSLT input file as seen in the preceding figure.   Note that there exist many tools that can take data in one format other than XML and produce XML output. These tools enhance interoperability and extend the life of legacy systems such that a smooth planned migration to XML based infrastructure can occur over a given period of time.

With the advent of XSLT 2.0, the original data source need not be XML. It can be an array of different formats such as comma separated value (CSV) file format (Hunter 2007). This was a major breakthrough in technological development and adoption of XML because only minor, more palatable changes in established organizational cultures is required. Therefore, translations are now a trivial process that may use a java applet, the proper implementation XSLT 2.0 set, or some other method.



FirstName	MiddleInitial	LastName	Rank	Service	Location	Status
John	Phineas	Doe	CAPT	USN	USS Bainbridge	Up
Peter	Demetrius	Jones	LCDR	USCG	USS Comanche	Up
Mathais	Plasidius	Montique	GS-15	DOD	Mombassa, Kenya	Up
Ameila	NMN	Starr	CIV	N/A	Fulton Co., GA	Deceased 99
Floyd	Morgan	Williams	CIV	Clergy	Boston, MA	Deceased 06
Tang	Vu	Chiang	CIV	N/A	Siagon, Vietnam	Up
Awanstar	Schaeffer	Lines	CIV	Contractor	Detroit, MI	Up
Eunice	Kennedy	Schriver	CIV	N/A	Monterey, CA	Deceased 09
Rovert	F	Kennedy	CINC	US	Washington, DC	Deceased 72
Ferdinand	Dubia	Cascinco	1st LT	USA	Ciaro, Egypt	Up
Geoffrey	Xavier	Parsons	SGT	LAPD	Los Angelos, CA	Up
Felipa	Cordoves	Kerr	CIV	N/A	San Diego, CA	Up
Christina	Sunshine	Johnson	CIV	USN Dependent	San Diego, CA	Deceased 90
Timothy	Antwoine	Cooper	GYST	USMC	Newport, RI	Up
Antonio	Steamer	Anderson	LCDR	USN	Baltimore, MD	Up
Vitterio	Julius	Crisp	CDR	USN	Sigonella, Sicily	Up
Julius	Von	Ceasar	CIV	N/A	Naples, Italy	Deceased 88
Loren	Jascupisco	Peterson	CIV	N/A	Beaumont, TX	Up
Eula	Janet	Praylor	CIV	N/A	Guam	Up
Adorn	Vanessa	Johnson	CIV	N/A	Manilla, Philipines	Up
Breanna	Naiomi	Santos	MAJ	USA	Muscat, Oman	Up

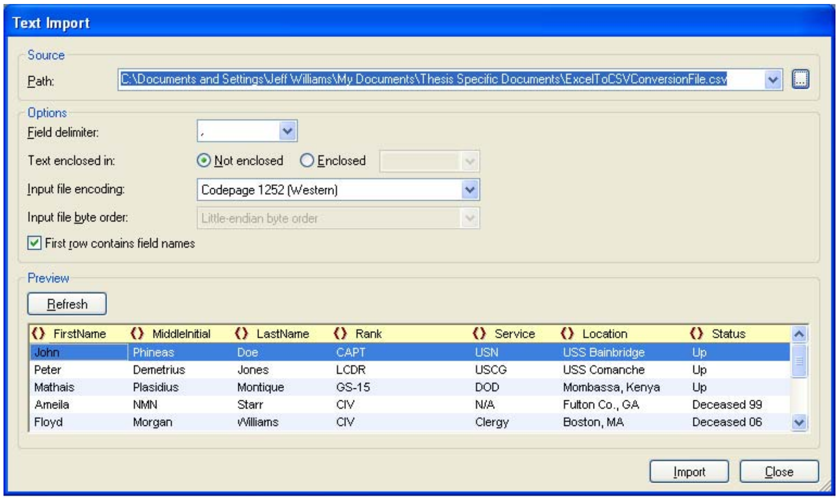
Table 3. The file above depicts a spreadsheet with an unknown native format.

Spreadsheets whose formats are unknown can generally be saved as comma delimited files ,otherwise known as Comma Separated Value (CSV) files. CSV files are simple text files in which each field is separated by a comma and each row by a carriage return. Most spreadsheets can read and output files in CSV formats. As such, there are several tools that can convert through the CSV or other files to produce an XML file. Altova XMLspy for PC based systems and Oxygen XML Editor for Apple Macintosh Systems are among several tools that are available. There are also a plethora of open source freeware and shareware resources available with functionality to support structured text-to-XML and XML-to-structured-text conversions. However, structured plain text, while occasionally convenient, can also be parsed by custom software. Structured plain text also remains significantly inferior to XML encoding since it cannot be validated and is further vulnerable to garble error.

```
FirstName,MiddleInitial,LastName,Rank,Service,Location,Status
John ,Phineas,Doe,CAPT,USN,USS Bainbridge,Up
Peter,Demetrius,Jones,LCDR,USCG,USS Comanche,Up
Mathais,Plasidius ,Montique,GS-15,DOD,"Mombassa, Kenya",Up
Ameila,NMN,Starr,CIV,N/A,"Fulton Co., GA",Deceased 99
Floyd ,Morgan,Williams ,CIV,Clergy,"Boston, MA",Deceased 06
Antonio,Steamer,Anderson,LCDR,USN,"Baltimore, MD",Up
Vitterio,Julius,Crisp,CDR,USN,"Sigonella, Sicily",Up
Julius ,Von,Ceasar,CIV,N/A,"Naples, Italy",Deceased 88
Loren,Jascupisco,Peterson,CIV,N/A,"Beaumont, TX",Up
Eula,Janet,Praylor,CIV,N/A,Guam,Up
Adorn,Vanessa,Johnson,CIV,N/A,"Manilla, Philipines",Up
Breanna,Naiomi ,Santos,MAJ,USA,"Muscat, Oman",Up
```

Figure 32. Comma Separated Value (CSV) file formats are one of many that XSLT can parse through. The CSV file above was created from a spreadsheet that may or may not have a native XML form.

For example, suppose that an organization’s data is contained in the format of a spreadsheet as in the Table 3. The data might be saved in the CSV file format (illustrated in Figure 32) to support being converted to XML with a given tool such as XMLspy, as shown in the Figure 33.



Text Import

Source

Path: C:\Documents and Settings\Jeff Williams\My Documents\Thesis Specific Documents\ExcelToCSVConversionFile.csv

Options

Field delimiter: ,

Text enclosed in: ● Not enclosed ○ Enclosed

Input file encoding: Codepage 1252 (Western)

Input file byte order: Little-endian byte order

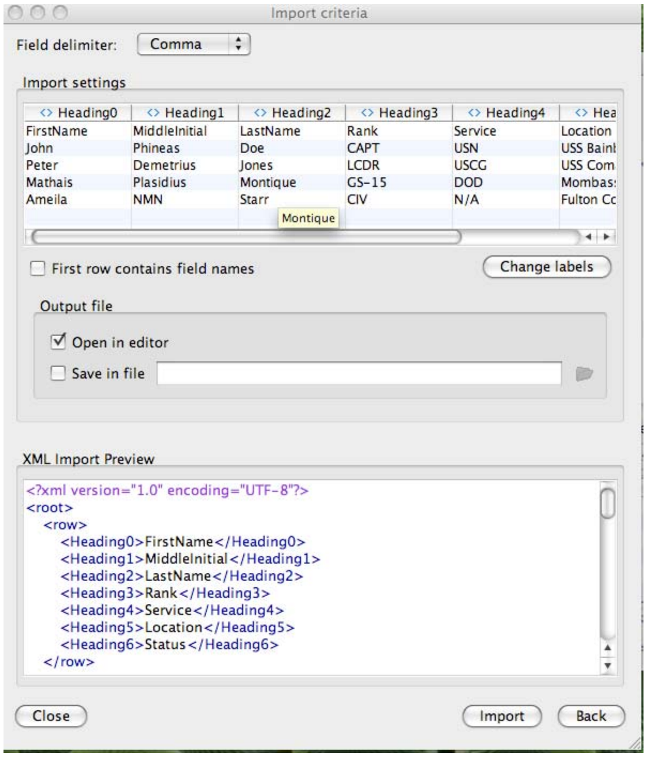
☑ First row contains field names

Preview

Refresh

FirstName	MiddleInitial	LastName	Rank	Service	Location	Status
John	Phineas	Doe	CAPT	USN	USS Bainbridge	Up
Peter	Demetrius	Jones	LCDR	USCG	USS Comanche	Up
Mathais	Plasidius	Montique	GS-15	DOD	Mombassa, Kenya	Up
Ameila	NMN	Starr	CIV	N/A	Fulton Co., GA	Deceased 99
Floyd	Morgan	Williams	CIV	Clergy	Boston, MA	Deceased 06

Figure 33. The CSV shown in the previous figure is processed using the XML Spy conversion tool.



Import criteria

Field delimiter: Comma

Import settings

Heading0	Heading1	Heading2	Heading3	Heading4	Hea
FirstName	MiddleInitial	LastName	Rank	Service	Location
John	Phineas	Doe	CAPT	USN	USS Bainl
Peter	Demetrius	Jones	LCDR	USCG	USS Com
Mathais	Plasidius	Montique	GS-15	DOD	Mombas
Ameila	NMN	Starr	CIV	N/A	Fulton Cc

□ First row contains field names

Output file

☑ Open in editor

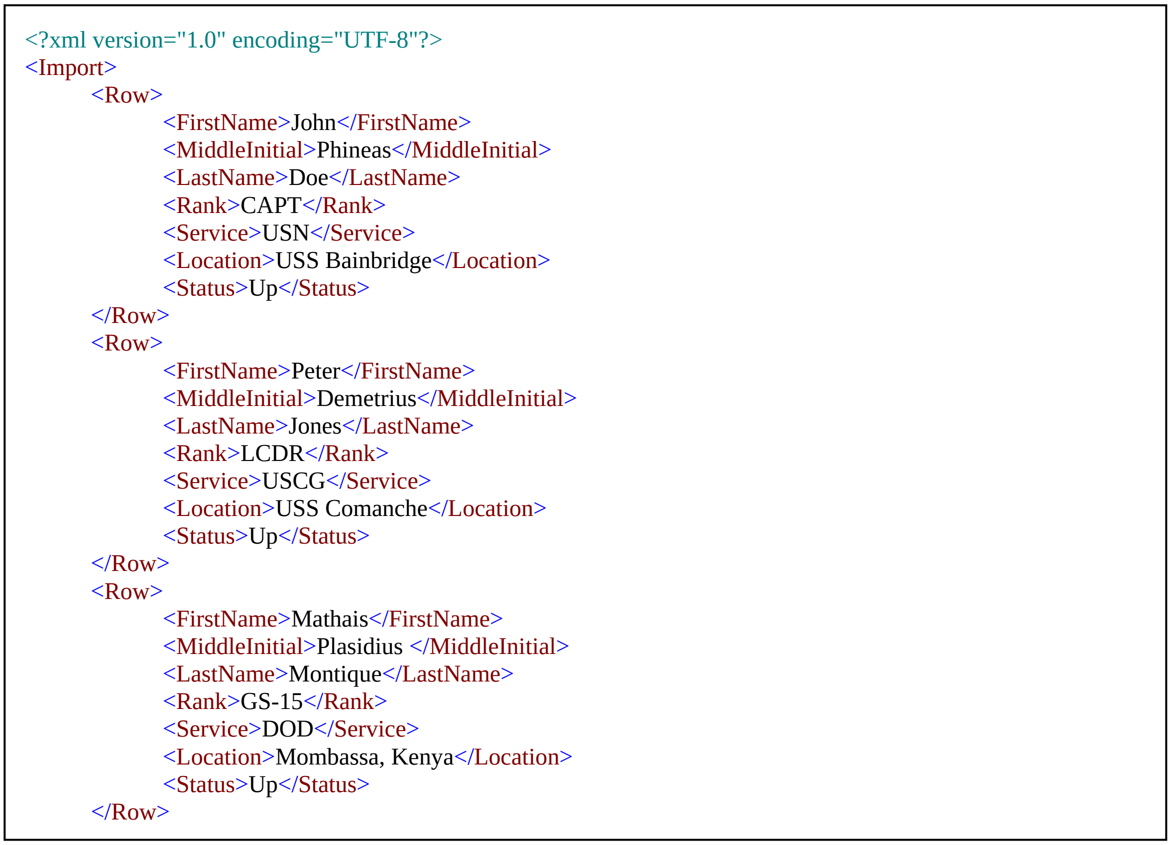
□ Save in file

XML Import Preview

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
   <row>
      <Heading0>FirstName</Heading0>
      <Heading1>MiddleInitial</Heading1>
      <Heading2>LastName</Heading2>
      <Heading3>Rank</Heading3>
      <Heading4>Service</Heading4>
      <Heading5>Location</Heading5>
      <Heading6>Status</Heading6>
   </row>
```

Figure 34. Several tools are available to convert files to XML compliant XML. This is a screen capture of Oxygen’s import tool designed for Apple Macintosh platform.

Depending on the tool used, the root of the output file may be different. The resulting file would be an XML file with the contents grouped by row each containing the elements FirstName, MiddleInitial, LastName, Rank, Service, Location, and Status as shown in the Figure 35.



```
<?xml version="1.0" encoding="UTF-8"?>
<Import>
	<Row>
		<FirstName>John</FirstName>
		<MiddleInitial>Phineas</MiddleInitial>
		<LastName>Doe</LastName>
		<Rank>CAPT</Rank>
		<Service>USN</Service>
		<Location>USS Bainbridge</Location>
		<Status>Up</Status>
	</Row>
	<Row>
		<FirstName>Peter</FirstName>
		<MiddleInitial>Demetrius</MiddleInitial>
		<LastName>Jones</LastName>
		<Rank>LCDR</Rank>
		<Service>USCG</Service>
		<Location>USS Comanche</Location>
		<Status>Up</Status>
	</Row>
	<Row>
		<FirstName>Mathais</FirstName>
		<MiddleInitial>Plasidius </MiddleInitial>
		<LastName>Montique</LastName>
		<Rank>GS-15</Rank>
		<Service>DOD</Service>
		<Location>Mombassa, Kenya</Location>
		<Status>Up</Status>
	</Row>
```

Figure 35. The generated XML data file can be viewed from the applications window. Above is a fragment of the output from the XML Spy conversion tool.

Alternately, for some ingenious individual, using an updated version of the SAXON engine, there exists XSLT 2.0 which supports direct conversion using regular expressions. In regards to the previous files, both XSLT 1.0 and XSLT2.0 can translate XML to another XML format or translate the file to the desired format. Consider the following, a human resources manager needs to provide a print out of her employees for a random Urinalysis screening. The administrator does not want to provide personally identifiable information (PII) to the requesting organization but provides the least amount of information required for them to complete their mission objectives. The administrator utilizes an XSLT such that only the rank and last name are generated as seen in the following example. The first step is to write the XSLT which is displayed in Figure 36.:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
<xsl:output method="xml" indent="yes" />
<xsl:template match="/">
        <Import>
                        <xsl:apply-templates select = "Import/Row/Rank" />
        </Import>
        </xsl:template>
        <xsl:template match="Rank">
                <Officer>
                        <xsl:element name="Rank">
                                        <xsl:value-of select="."/>
            </xsl:element>
                        <xsl:element name="LastName">
                                <xsl:value-of select="../LastName"/>
                        </xsl:element>
                </Officer>
        </xsl:template>
</xsl:stylesheet>
```

Figure 36. The XSLT file above translates the XML file to a streamlined format to obtain rank and last name elements.

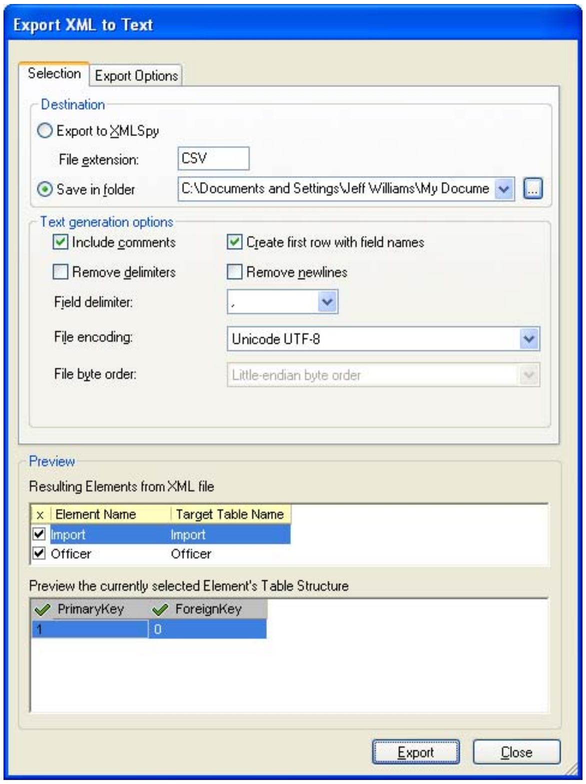
The resulting XML output file would appear as in Figure 37.

```
<?xml version="1.0" encoding="UTF-8"?>
<Import>
    <Officer>
        <Rank>CAPT</Rank>
        <LastName>Doe</LastName>
    </Officer>
    <Officer>
        <Rank>LCDR</Rank>
        <LastName>Jones</LastName>
    </Officer>
    <Officer>
        <Rank>GS-15</Rank>
        <LastName>Montique</LastName>
    </Officer>
    <!—additional rows and data omitted →                .
    <Officer>
```

Figure 37. The output of an XSLT is in a customized format in contrast to the original. Since all of the data was not required it simply printed only that which was asked. The file is now ready to be processed by any tool that needs this format.

By performing transformation in this manner, it is possible to convert data in a variety of formats such that it satisfies the requirements for XML well-formedness, and

XML validation such that XML C14N, digital signature, and XML encryption can follow. On the aft end of the transmission, the message is decrypted, digital signature and message digest verified, and output file is eligible for display or further manipulation. If the output file requires further conversions to match the recipient's data format, either an XSLT or a conversion tool such as XMLspy can be used to convert to the appropriate format. Figure 38 shows the conversion of the output file from and XML file to a CSV file.



Destination

○ Export to XMLSpy

File extension: CSV

● Save in folder C:\Documents and Settings\Jeff Williams\My Docume

Text generation options

☑ Include comments ☑ Create first row with field names

☐ Remove delimiters ☐ Remove newlines

Field delimiter: ,

File encoding: Unicode UTF-8

File byte order: Little-endian byte order

Preview

Resulting Elements from XML file

x	Element Name	Target Table Name
☑	Import	Import
☑	Officer	Officer

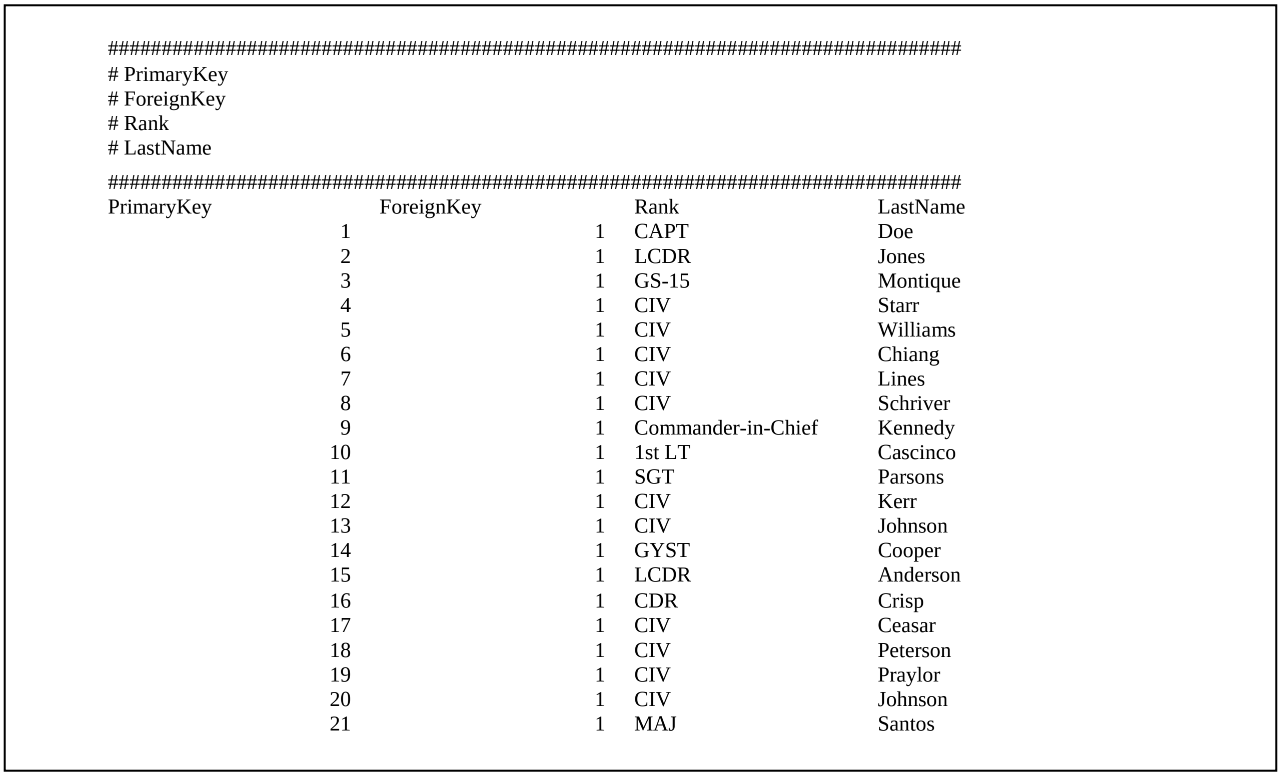
Preview the currently selected Element's Table Structure

✓ PrimaryKey	✓ ForeignKey
1	0

Figure 38. XMLspy is equipped with tools to convert XML files to other formats such as CSV as illustrated in this figure.

The resultant file of the conversion follows, which requires minor modification to be compliant to the database or spreadsheet system that uses the information. It is listed in the Table 4.

Thereafter, the file can be opened with MS Excel or any other application that accepts data in CSV file format, as displayed in the Table 4. This is a SQL Table.



```
####################################################################################
# PrimaryKey
# ForeignKey
# Rank
# LastName
####################################################################################
PrimaryKey              ForeignKey           Rank                  LastName
                     1                    1  CAPT                  Doe
                     2                    1  LCDR                  Jones
                     3                    1  GS-15                 Montique
                     4                    1  CIV                   Starr
                     5                    1  CIV                   Williams
                     6                    1  CIV                   Chiang
                     7                    1  CIV                   Lines
                     8                    1  CIV                   Schriver
                     9                    1  Commander-in-Chief    Kennedy
                    10                    1  1st LT                Cascinco
                    11                    1  SGT                   Parsons
                    12                    1  CIV                   Kerr
                    13                    1  CIV                   Johnson
                    14                    1  GYST                  Cooper
                    15                    1  LCDR                  Anderson
                    16                    1  CDR                   Crisp
                    17                    1  CIV                   Ceasar
                    18                    1  CIV                   Peterson
                    19                    1  CIV                   Praylor
                    20                    1  CIV                   Johnson
                    21                    1  MAJ                   Santos
```

Table 4. The use of tools may require further tweaking of the resultant file to get it in the appropriate data format to be used by the system of choice.

Unlike XSLT 1.0, XSLT 2.0 supports direct up-conversion from a text based source to XML which means that no other tools are required. Up-conversion refers to the generation of a format with detailed markup from a format with less-detailed or no markup, where it is necessary to generate the additional markup by recognizing structural patterns that is implicit in the textual content itself (Kay 2009).

The aforementioned discussion represents the flexibility of XML as a viable tool that can be rapidly adopted and implemented with existing systems with minimal learning curve. The variety of acceptable source and corresponding output data files from an XSLT contributes to XML rapid acceptance by national and international groups. This in turn allows the discussion to focus to be placed upon the processes required for providing secure communications with non-repudiation via digital signature and XML encryption.

The world is in a constant state of change which means that organizations that seek to maintain their information superiority affordably need to seek out and adopt web based technologies that require little or no change to their network architecture. The application of XML Encryption and Authentication is one of many possible solutions to achieve this goal. By utilizing digital signatures, secure hashing algorithms, compression and encryption techniques; it is possible to provide adequate security for perishable pertinent information. Perishable information is data that is valid for a brief period of time such as ship or personnel global positional data.

D. DIGITAL SIGNATURE

A digital or electronic signature is a cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation (CNSS Glossary Working Group). XML Signatures provide all of theses features as defined by XML Signature Syntax and Processing (W3C XML Security Specifications Maintenance Working Group 2008 Second Edition). On June 30, 2000, the U.S. Congress enacted the Electronic Signatures in Global and National (ESIGN) to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically with special requirements for businesses via section 101(c)(1) of the Act (Federal Trade Commission and Department of Commerce 2001). Thus an electronic signature holds the same weight as a written signature. Therefore, as specified within the definition there exists a method to ensure that neither the signature is forged nor the document altered. This is accomplished by running the document through a mathematical hashing algorithm to obtain a reproducible fingerprint (Message Digest) of the document combing the message digest with the entity’s private digital certificate to encrypt the message digest to generate a unique signature. Thereafter, the signature is appended to the document, which is unique to both the user and the document. When the document is received at the point of destination, the recipient of the document can validate the identity of the sender by decrypting the digital signature with the sender’s public key and compare the document’s fingerprint with the computed has of the document. If the message digests match and there exist a trusted third party, the

Certificate Authority (CA), which can verify the authenticity of the signer, then there can be no doubt that it was indeed the sender that sent the document. The validated digital signature assures signer authenticity, accountability, data integrity, and non-repudiation of the electronic document.

Non-repudiation is the assurance the sender of data as provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data (CNSS Glossary Working Group). To completely satisfy the CNSS definition of non-repudiation there must also be a means to assure the sender of data proof of delivery so neither can later deny having processed the data. It must be noted that the use of a digital signature alone is not enough to protect the document during transmission from point A to point B. It nevertheless remains sufficient to validate that the document was sent by a specified entity.

XML digital signature contains several processes as depicted in the following figure. Each document must be well formed. A well-formed XML document complies with the syntax rules contained within the XML specifications. Any deviations, however slight, makes the document invalid. Within XML compliant browsers, editing tools, and compliant software, there exist an XML parser that checks to ensure that the file is valid. Invalid XML files are usually rejected and therefore not displayed. After XML validation, the document is processed to be represented in a standard canonical representation.

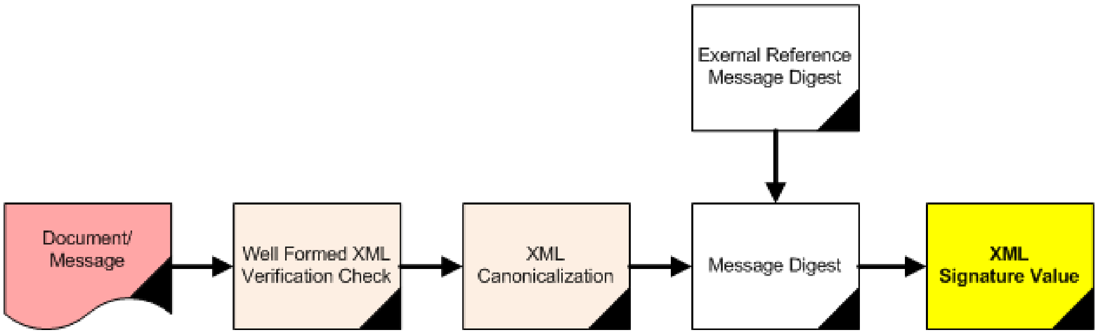


Figure 39. Basic function flow path for XML Digital Signature from document generation to signature creation.

1. Canonicalization (C14N).

During XML canonicalization (C14N) all non-essential characters are removed to include white spaces. The acronym C14N comes from the number of characters between the C and the N in the word Canonicalization: Forteen. There is more than one method of performing canonicalization. X3D-Edit specifies two methods: XML C14N and X3D-Edit C14N. The most distinctive difference between the two methods is that with X3D-Edit C14N empty elements are converted to singletons, whereas, XML C14N will ensure that for every opening tag, there is a corresponding closing tag. For more information on XML canonicalization, visit the World Wide Web Consortium Web site and review the technical specification at http://www.w3c.org/TR/xml-c14n.html. By performing the process of canonicalization, the document generated is representative of that produced by other canonicalization processes on other systems. A document in canonical form may be substituted for the original document without any loss of generality. Canonicalization is a critical piece to attaining universal interoperability with systems of various origins.

2. Message Digest

Once the document has been canonicalized, a message digest of the document and all associated documents referenced within the main document must be computed. A message digest is the product of a unidirectional mathematical function that takes a variable length input string (document) and converts it to a fixed-length output string (hash value / message digest) (Schneier 1996 p. 30). With the XML digest process both internal and external digests are computed to derive a hash value that is unique to that particular document. The value generated is used only once and large enough such that it cannot be reproduced.

If a digitally signed document is sent in the clear without any other form of protection, the XML digital signature *does not* guarantee the confidentiality of the document. The document is susceptible to interception by devices or applications such as *wireshark, airsnort*, etc. (The Schmoo Group 2009 Retrieved August 2009, Combs, Retrieved August 2009). For the intent of this thesis, it is assumed that the hashing algorithm used does not produce two message digests that are equivalent to each other but that each hash is unique to that particular document.

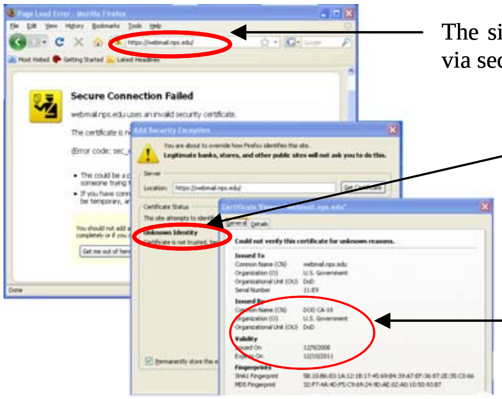
This information is in turn passed to the XML signature generation process. The digital signature process encrypts the message digest with a unique private key ensuring message integrity and sender non-repudiation. When the recipient receives the document, he/she computes a message digest using the same algorithm as was used in its generation and compare that result with the message digest decrypted with the public key.

In order to ensure compatibility across the board, all systems need to meet the minimum requirements for digital signature. Although it does not grant confidentiality, the assurances provided when properly implemented satisfy the majority of the information assurance requirements previously discussed. Strict adherence to the W3C standards is key to successfully producing an interoperable XML document that can be processed by multiple agencies and by national assets of various countries. Its open source and non-proprietary, which means no organization can legally lay claim to the ideas, which in terms makes it an appealing architecture for budget conscious organizations which can grow their own tech support infrastructures and obtain reachback support via online communities, newsgroups, IRC chats, etc. The W3C community forum is an excellent source of information that may be appropriate for several Web-based specialist supporting an organization. Others may elect to purchase a service from on-call professionals particularly skilled in the open source technology for a fee.

3. Identity Management

Digital signature technology offers the opportunity to investigate identity management. Too often the technology employed is encumbered by warnings and pop-ups that act as an annoyance to the average end user. Over time the user looses their security awareness and just click on the dialogue to quickly move to the next task. In so doing, the user’s apathy may invite the opportunity for an attacker to infiltrate the network. XML digital signature in concert with modern browser technology can help in communicating in a user-centric, user-friendly, environment the authenticity of the sender such that the content can be trusted.

A user-centric approach incorporates techniques and skills of human-system integration specialist such as those used in the construction and operation of the apple Macintosh computer and operating systems. The approach focuses on how the computer can provide information to the user in a more usable fashion. Consider the scenario of a user requesting a document from a Department of the Defense server, as shown in Figure 40.


Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://webmail.nps.edu/
Most Visited Getting Started Latest Headlines
Done
Add Security Exception
Get Certificate
General Details

Secure Connection Failed

webmail.nps.edu uses an invalid security certificate.

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://webmail.nps.edu/

Certificate Status

Unknown Identity
Certificate is not trusted,

Could not verify this certificate for unknown reasons.

Issued To
Common Name (CN) webmail.nps.edu
Organization (O) U.S. Government
Organizational Unit (OU) DoD
Serial Number 11:E9

Issued By
Common Name (CN) DOD CA-18
Organization (O) U.S. Government
Organizational Unit (OU) DoD

Validity
Issued On 12/9/2008
Expires On 12/10/2011

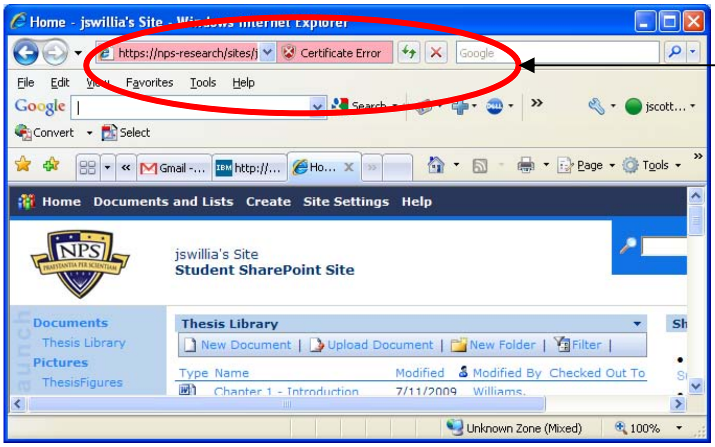
The site Naval Postgraduate School secure website for webmail via secure sockets layer

Firefox has notified the user that the site has failed because the identity of the server has not been validated by a trusted/ recognized authority

Certificate information showing a valid certificate offered provided by the United States government

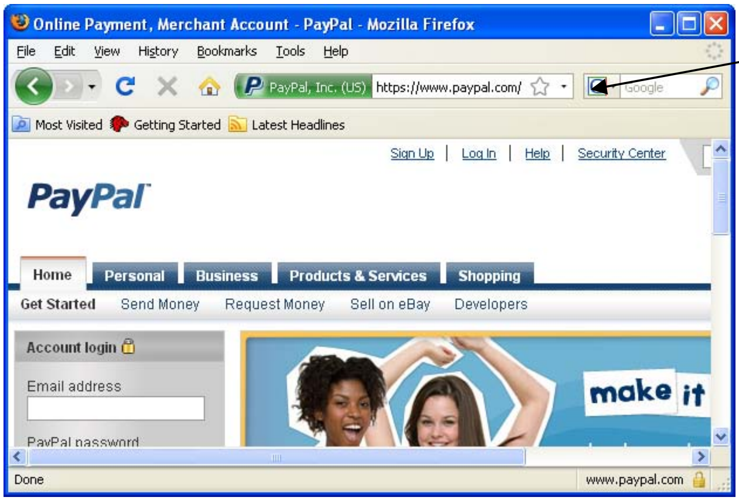
Figure 40. Browsers employ different mechanisms to assist the user in protecting personal identifiable information. The figure above illustrates Mozilla Firefox implementation of identity management by having the user decide whether the site is trustworthy via certificate verification.

Without access to the certificate authority (CA) database, a trust relationship cannot be established. Therefore, the user must ultimately determine the trustworthiness of the Web site. Browser awareness can assist in alerting the user of a potentially dangerous situation without negatively impacting the user experience. The use of colors, such as red, within the browser bar denotes proceed with extreme caution, as seen in Figure 41.


Home - jswillia's Site - Windows Internet Explorer
https://nps-research/sites/j
Certificate Error
Google
File Edit View Favorites Tools Help
Google
Search
jscott...
Convert
Select
Gmail -...
http://...
Ho...
Page
Tools
Home Documents and Lists Create Site Settings Help
NPS
jswillia's Site
Student SharePoint Site
Documents
Thesis Library
Pictures
ThesisFigures
Thesis Library
New Document | Upload Document | New Folder | Filter |
Type Name Modified Modified By Checked Out To
Chapter 1 - Introduction 7/11/2009 Williams
Unknown Zone (Mixed)
100%

Internet Explorer indicating a certificate problem

Figure 41. Internet Explorer warns the user at the command bar of possible invalid certificate. Keep in mind that the user still has full control as to whether or not he/she precedes to the site.



Displays extended validation of this Versign protected site. Green means go!

Site is secure

Figure 42. Mozilla Firefox is displayed the PayPal site as secure by verifying its identity in which its logo is within the address bar the color is green for go and there is a lock-&-key representing a secure Web site.

The use of colors and symbols shows a visual flag to enhance the user’s situational awareness, to include revealing the accountable party and the identification of the trusted organization that issued the certificate without detracting from the user’s web based browsing experience. The padlock immediately alerts the user to the site’s trusted nature by a central authority to which the browser application has access to verify the source identity. If both the certificate is valid and the document is secure for web services, then both the padlock, the credentialing authority, and the toolbar color illuminates the change. XML digital signatures provide identity management because only the author has custody of his/her private key for signing a document. As seen in Figures 41 and 42, the information is displayed in an unobtrusive manner consistent with the alerts the user is communicating with a secure document or receiving a secure transmission from an identified source. Therefore, within the scope of the aforementioned, accountability is placed with the certificate authority (CA), as it is the central authority that validates the identity of the sender. SSL based transactions are denoted by a lockbox within the browser. Certificate endorsement is crucial to establish a sufficient ring of trust. Since anyone having the proper software and equipment can generate a certificate, the certificate authority must be trusted by both sender and originator else no trust relationship exists. This is a matter of proving identity. *The DotCrime Manifesto* speaks about the concepts of identity management and of the initiatives that multiple proprietary and open source companies are undertaking to implement it.

Within the scope of this topic, identity management comes in the form of a digital signature. Digitally signed documents and the respective ordering of encryption-signature-compression is critical to ensuring that the document's point of origin is authentic. Again, it must be iterated that the term, security, in the sense used herein is focused from the secure endpoint to secure endpoint. All transmissions and transports are potentially insecure.

Communications with multinational military organizations and civilian agencies alone is not sufficient to successfully accomplish the mission of international interoperability. The oceans are used by commercial, military, and civilian pleasure vessels (yachts, sailboats, fishing boats, etc.). As such, there exists a need to exchange data, track information, and status with the civilian craft. Bridge-to-Bridge radio communications has been the method by which information has been exchanged for several years. Now with the threat of piracy on the rise, this method needs to be augmented by data exchange technology such that any military or law enforcement vessel can quickly send assets to the problem area to offer a would-be aggressor an incentive to rethink their intentions. The world is no longer seen as havens of democracy, fascism, or communism that protect its citizenry from piracy. The view has changed out of necessity because no single nation can have its forces transcend space and time to be on station during an attack upon its citizenry while at sea. Such actions require collaboration amongst traditional and nontraditional partners to get the job done.

Suppose a United States flagged warship *ALPHA* receives a distress message from a civilian vessel, *BAKER* that is 50 miles away. The distress message has a universal code that signifies an pirate attack is in progress. Even at flank speed the U.S. flagged vessel would arrive after the damage had been done. However, it is noted that another ship *CHARLIE* in which no formal agreement is on file is within 15 miles of the scene. At flank speed and with aerial assets it may be able to avert the attack and detain the suspected pirate vessel. Ship *ALPHA* decides to initiate a secure communications exchange with ship *CHARLIE* in support of non-military unit *BAKER*. Unit *BAKER* is neither ofU.S. nor ship *CHARLIE* origin, but pirates are attacking it. Since the host nations of Ship *ALPHA* and Ship *CHARLIE* lack a formal agreement in regards to secure secret communications, there must exist an alternative method to securely communicate and exchange information without alerting the pirates. Bridge-to-Bridge communications can be intercepted since it is sent in the clear which may be monitored by the pirates and thus potentially provide them with an early warning mechanism. A method of establishing a viable and secure communication path is to utilize World Wide Web Consortium (WC3) standardized based XML encryption and authentication protocols. It is assumed that the problem of key distribution has been resolved and both *ALPHA* and *CHARLIE* has access to each other's public key. Ship *CHARLIE* is closer but lacks pertinent data that Ship *ALPHA* possesses. Therefore, Ship *ALPHA* initiates voice communications to Ship *CHARLIE* such that they can be on the alert for an electronic transmission. Ship *ALPHA* generates the XML document, computes a message digest using secure hash Algorithm (SHA1) and digitally encrypts the message digest with its private key. Now the document along with the digital signature are compressed and encrypted with Ship *ALPHA's* private key. It is afterwards encapsulated and transmitted to Ship *CHARLIE* with secure sockets layer (SSL). Ship *CHARLIE* utilizes Ship *ALPHA's* public key to decrypt the message and verify that it was indeed from Ship

ALPHA. It afterwards decrypts the message digest and compares it with the computed hash. They match! Now the XML document is translated and imported into Ship *CHARLIE's* database such that they can take appropriate action against the confirmed pirates to include pursuit into coastal waters barring international agreements until a proper handoff can take place. The secure exchange of information between Ship *ALPHA* and Ship *CHARLIE* whose internal systems were indeed dissimilar would have resulted in the capture, detainment, and subsequent arrest followed by extradition of the pirates such that they may be tried by the host nation to which they committed the offense. Thus, a win-win scenario envelopes such that the world is less one threat to piracy, both Ship *ALPHA* and Ship *CHARLIE* receive credit for their contributions leading to the capture of pirate ship *FISHER* and the country which held legal arrest authority can show its people that it is taking a proactive stance against piracy by cooperating with both traditional and non-traditional international players in keeping their coastal waters secure without giving up their sovereignty. Upon accepting custody of the alleged pirates, Ship *CHARLIE* transmit all data relating to the act to Ship *ALPHA*, and also to the respective country officials using the same secure means as previously described. Naturally, both Ship *ALPHA* and *CHARLIE* forwards a synopsis of events to their respective officials using approved secure means and promptly depart for international waters as the task has been completed.

Upon further analysis of the scenario described above, it was void of the apparent military standard Mandatory Access Control (MAC) for the encryption and decryption of the document. What was employed was the Discretionary Access Control (DAC) in which the originator made a decision as to which entities needed to receive and decrypt the information. Therefore, a socially generated trust relationship is developed between sender and recipient such that both parties acknowledge that they shall not misuse and/or abuse the privilege of viewing, processing, and disseminating the information to other parties. However, by using DAC the originator no longer has control over the information sent to the recipient. The recipient further process and distribute the information, which is why the information sent via this means must not carry a classification higher than controlled unclassified information (CUI). The DAC protocol is discussed in more detail in later sections of this document.

In contributing to the efforts of creating a comprehensive national security strategy for cyberspace, fostering the public-private partnerships, military-civil coalitions, authenticate digital identities, and taking the lead in developing a framework for acquisitions, utilization of a standards based approach to document-level XML encryption and authentication for sensitive unclassified communications guarantees a multinational cost effective solution to an ever evolving net-centric environment. The major issues confronting several organizations desiring to exchange information may be lack of infrastructure to exchange data dynamically with cooperating partners, identity management, and the threat of providing an avenue for malware to propagate throughout their respective network. Trust relations established amongst familiar organization are a step in the right direction. However, in certain environments such as coalition partnerships amongst nations in which no formal treaty and where the expeditious nature of communications determines the outcome of a potentially hazardous situation, it may not be prudent to establish a system-high trust relationship. Therefore, communications take place over the unclassified network. Nonetheless, sensitive but unclassified communications still require a level of security commensurate with the information contained therein. To this extent, there must be a mechanism in place such that messages can be passed between to the partners with minimal exchange of technology.

The term Document-Centric Security is a unique concept. Instead of solely focusing on the system and network architecture, it focuses on the securing information content within the document itself. This concept coupled with XML security and authentication augments the security posture an organization and prepares a path for the implementation of a Discretionary Access Control policy on the document within the constraints of the organizational security policy. The compression, digital signing and encrypting of the document afford the originator and recipients a measure of assurance that the confidentiality, integrity, the authenticity of the message is maintained. Therefore, it is highly plausible to provide document-level framework for dynamic security requirements for unclassified but sensitive material.

Dynamic communications is often times referred to as on-the-fly communications. It refers to the dynamic establishment of time sensitive electronic communications due to urgent matters or affairs within or around the immediate environment or area of operations (e.g., During the Katrina Humanitarian Assistance Disaster Relief Effort hastily formed networks were established to connect volunteers, civil and military entities to support theU.S. citizens of Louisiana.). Over the last few years, there exist an increase multinational and/or multi-agency collaboration around the globe. This trend extends beyond military organization and quite possibly may be the basis for current and future terrorist/hostile cells throughout the globe. Both economic health and the need for each nation/corporation to safeguard their national interest against asymmetric threats have prompted a global response for short and long term cooperative operations. Thus, there exists a need for a secure framework that can securely exchange message-based based information with traditional and non-traditional partners without significant lockstep hardware or software requirements. XML documents shared dynamically as messages must be accessible to each specific site without compromising the integrity of the document. To achieve this objective, encryption and authentication must be performed in concert with compression techniques.

E. DISCRETIONARY ACCESS CONTROL (DAC)

A discretionary access control (DAC) policy is a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. DAC is based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. In accordance with the Department of Defense 8500.2, DAC is sufficient information assurance mechanism to interconnect information systems operating at the same classification but with different need-to-know rules. To interconnect between DoD and non-DoD systems a controlled interface is required. This brings us back to the concept of employing Document-Centric Security and transmitting the data from the unclassified enclave to unclassified enclave without digitally signed, compressed, and encrypted such that when opened within the virtual machine of the host system, the data can be viewed in a secure fashion by authorized personnel. Although this paper does not delve into the virtues of virtual machines, the author highly recommends their use in regards to minimizing potential damage or system infections. If the message is either generated or read on an infected machine, a virus may potentially propagate. It is recognized that discretionary access control implementations are prone to Trojan Horse attack. A Trojan Horse is malicious code that appears benign to the user. It may be in the form of a game, a photographic image, or streaming video. However, once loaded the Trojan Horse may commence its attack with inherited system access rights as the user. Additionally, the user may not be able to discern if there is any malfeasance because the Trojan may access the disk with every disk access of the user or log all keystrokes and send them back to the attacker. However, if constrained with rights on a virtual machine whose user rights are less than the owner's rights; widespread infection can potentially be contained to the virtual machine. For more information on virtual machines see Pokek paper entitled "Formal Requirements for Virtualizable Third Generation Architectures" (Pokek 1974).

F. PIRACY CASE STUDY

1. Piracy

Piracy is a war-like act committed by a non-state actor, especially robbery or criminal violence committed at sea, on a river, in the air above the seas. The act is committed outside the jurisdiction of any nation and without the authority from any government (Encarta Encyclopedia). Under article 100 of part VII of United Nations Convention on the Law of the Sea (UNCLOS) all States shall cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State. On the high seas, or in any other place outside the jurisdiction of any State, every State may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board. The courts of the State which carried out the seizure may decide upon the penalties to be imposed, and may also determine the action to be taken with regard to the ships, aircraft or property, subject to the rights of third parties acting in good faith (Pokek 1974). The language within the UNCLOS makes it quite difficult to bring pirates that seek out prey in international waters and upon completion of the act retreat to coastal waters. UNCLOS defines a warship as a ship belonging to the armed forces of a State bearing the external marks distinguishing such ships of its nationality under the command of an officer duly commissioned by the government of the State and whose name appears in the appropriate service list or its equivalent, and manned by a crew which is under regular armed forces discipline. As such, there is a requirement for ships to expeditiously handoff vital information and obtain approval to continue the pursuit of the pirate vessel and/or aircraft in which all states maintain their sovereignty and the criminals are brought to justice. An increase in bureaucracy is counter to the solution sought. However, using a standards based approach to securely pass perishable information from the set A = {military, national agency, law enforcement, government entity} to a set B = {military, national agency, law enforcement, government entity} regardless of nationality with each entity having dissimilar systems XML encryption and authentication can bridge the gap. To facilitate the exchange a trust relationship must be established between the participants such that each player has access to the others public key to verify their identity. Additionally, the secure hash algorithm must be known to verify the integrity of the document. In situations in which there are no formal agreement between A and B, it is critical that both entities possess a means of identity management such that both sender and receiver can verify the identity of the other. Upon validation of the document integrity and the identity of the sender, the receiver can take appropriate action in regards to hot pursuit and detainment of suspected pirates until law enforcement officials arrive.

Some of the issues regarding piracy are the following:

- Automated Communications. There must be some form of internationally recognized mechanism aboard civilian and commercial craft to report the act an act of piracy in progress to include basic information such as geolocation data, unit name, time and date stamp, base course and speed. The automated communications alerts military and civil authority of the problem quicker such that the probability of capturing the suspects increases. It allows capable units to vector in on the suspected location and deliver assets to support the victim.

- Standardized Communications Protocols. Dissimilar systems must be able to securely exchange data between one another with minimal transfer of cryptographic technology and associated hardware.
- Legal Liability. A nation may be held liable for the loss of review of legitimate businesses if the court finds that there is insufficient evidence to support detainment and/or seizure of craft and personnel suspected of piracy.

Modern piracy may not be an overt act clearly visible from sea, air or shore. Therefore, the laws themselves restrict law enforcement and military vessels from taking immediate action on suspected pirates.

Automated emergency communication that electronically sends geolocation and identity data via the use of digital signatures and XML Authentication alerts cognizant entities and organization that illicit acts are occurring and paves the path for international and littoral direct support without overtly alerting the suspects that are committing the offense. This in turn reduces the time the pirates have to orient, observe, decide and act (OODA). By disrupting the pirates' respective OODA loop by increasing the response time via multicast transmission to capable units, the cognizant authorities can make their case, detain the crew of the suspected vessel, and make subsequent arrests as warranted.

G. SUMMARY

Securing sea lines of communications in today's world extends beyond the borders of a single nation and requires both multiagency and multinational support and cooperation. However, trust is of a major concern to all organizations and entities facing the engaged in operations. Other issues include but are not limited to confidentiality, message integrity and verification, as well as message authentication. The result of the merging requirement is the extension and execution of an open source international standard employing extensible markup based languages and translation services to render an unbiased secure communications infrastructure.

Piracy is a threat to the international community but working towards a single consolidated goal with multiagency and multinational traditional and nontraditional partners, the threat can be minimized. Using XML enables even those that do not currently play work together swiftly assimilate into a cohesive organized unit with a robust secure communication mechanism to pass critical data.

V. EXEMPLAR APPLICATION CAPABILITIES

A. INTRODUCTION

Stable secure communications do not happen by chance. It requires proper planning prior to execution. Therefore, in looking at the day-to-day operations of a multinational force, it is critical to first examine the level of planning that went before it. Whether things go according to plan or not, the base plan serves as a point of reference for ongoing and future evolutions. The XML specification provides the blueprint for system design that facilitates the exploration of various implementations to achieve security. This allows the open source community to evaluate the recommended and future goal for the most efficient operation of an XML-based security solution, which can be illustrated by operational examples.

1. Day-to-day Communication Exchange Between Nations

Everyday afloat and ashore data is exchanged between coalition, multinational, and multiagency partners in efforts to achieve a common goal. Although these players work together, they are apprehensive of the other. The story of the how Troy fell resounds with data exchange. History states that the Greeks left a wooden horse at the gates of Troy after years of fighting. The Trojans pulled the horse into its city. However, within the wooden horse hid the Greek warriors. They eliminated the opposition opened the gates and the Greek army took the city. Software developed by a single country faces the same issue as the Trojan horse. There is no way to ensure that it is devoid of back doors or other glitches that may be used in an adversarial manner. Therefore, open standards-based technology is the key to overcoming this Trojan horse scenario because each country is able to build its own solution that is interoperable with any other that utilizes the standard.

By utilizing an open standards-based solution, secure communication exchange with joint, coailition, and multinational partners are possible with a high level of assurance because the technical implementations are grown and developed within country based upon international standards such as those provided by the W3C for XML which is already adopted in several commercial products. The use of open source standards-based technologies promotes interoperability between dissimilar systems operating on various platforms.

Interoperability is a key factor whenever data exchange is required especially with unknown or new participants.   Whenever interoperability for data exchange fails or is not plausible it must be passed by radio, semaphore, or other method, which may require the partners to be closer than that which is comfortable such as two afloat units that have never practiced with one another sailing abreast each other at distances of under 1000 yards.   If one ship makes a mistake then a collision at sea might occur. It only takes a few moments when ships are operating in close proximity to one another.

The combinations of voice enhanced by data intechange reduces time lag and increases the accuracy of information passed. Various flavors or XMPP Chat can be used to enhance communication between participants. With XMPP Chat anyone can establish a communications server and other can join. The partners would still utilize voice communications that would vbe supplemented by XMPP chat such that an official log of the communications exist that can be referred back to at a later date. XMPP Chat can be supplemented using either Security Assertion Markup Language (SAML) while implementing each message as an independent document with encrypted elements. The micro message would be decrypted and decompressed on the recipients location but this may cause additional delay in processing the information to the screen because additional CPU cycles are required for each encryption and each decryption of the information contained.

SAML enables single sign-on such that each client node logs into a single site and have the ability to log onto other systems that are tied to that client's associated credentials. XML Security supplements this technology such that the recipient has additional assurance that the document is authenticated and unaltered via the use of XML digital signature. Enhanced confidentiality can be achieved through the use of XML encryption. This assures that even with application of SAML, documents are available only to those personnel and entities available with the appropriate credentials.   This futher assures that the person accessing the information has a valid need-to-know, by two-factor authentication—successful access via SAML and the possession of the appropriate certificate.

Two entities that lack a current formal agreement need to communicate with one another. However, the only record of their communications exchange is in a bridge-to-bridge logbook in which the operator records short hand notation of information passed. Vital information may be lost, recorded in error, or misinterpreted by either party.

B. SCENARIO MESSAGE-TYPE REQUIREMENTS

1. Requirements

Although XML is a structured language, there is no general requirement for the structure of one message or document to be the same as another structure. However, to obtain interoperability the structures the XML schemas that are in use must be available to convert the format between the various flavors of XML. The base requirements that must exist for all XML messages processed using XML signature and XML encryption are:

- XML messages must be well formed.
- XML messages must be valid.
- XML messages must be canonicalized when implementing XML encryption

If the base requirements are satisfied, then any XML-based document format can be translated to any other XML-based document format via an extensible stylesheet language transformation (XSLT). This feature in addition to the application Unicode makes XML a universal language that breaks down barriers inherent with spoken languages. Unicode is a character code that defines every character in most of the speaking languages of the world. It does this by associating each character with a specific number (The Unicode Consortium). All tools that support use UTF-X are Unicode compliant.

C. SIGNED, ENCRYPTED, AND COMPRESSED DOCUMENTS

1. Use Cases using XML Signature, XML Encryption, and Compression

There are various approaches for applying the World Wide Web Consortium specification for XML Signature, XML Encryption, and Compression. Figure 44 shows a suboptimal use case that achieves XML digital signature, encryption and EXI compression.

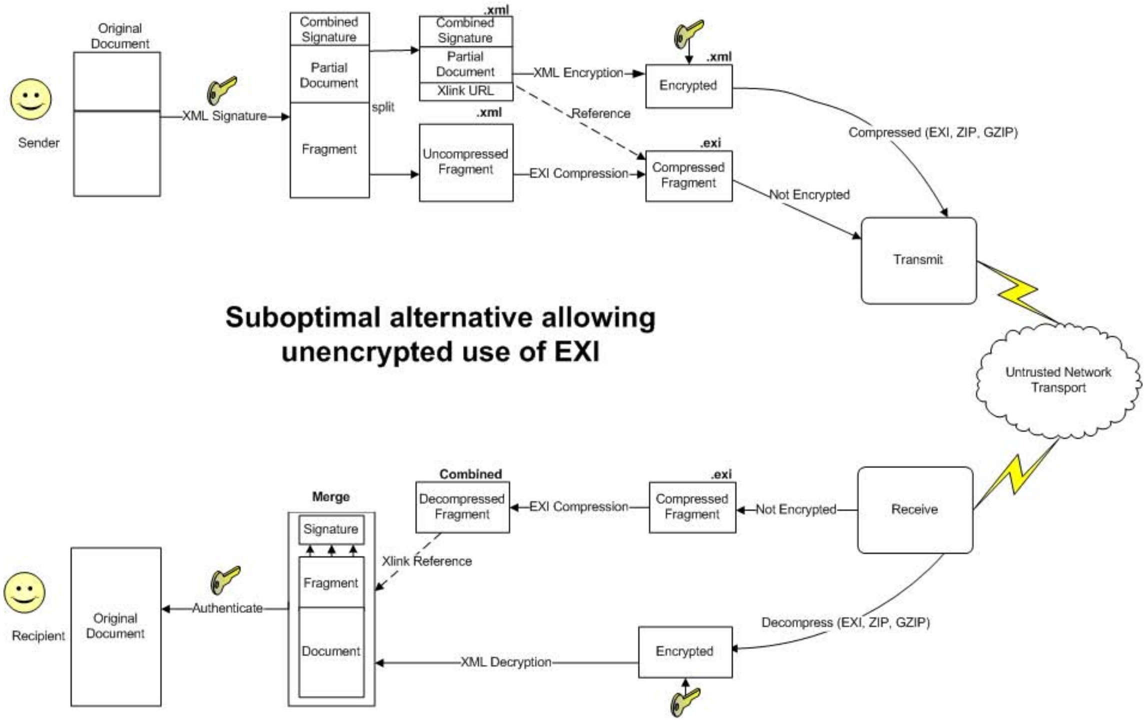


Figure 43. XML files can be fragmented and maintain its XML authentication attributes when put back together. Although recommended, the entire document does not need to be encrypted.

Due to the verbose nature of XML, it is considered more costly than other methods of data transfer. However, by applying compression techniques that are compatible with the W3C efficient extensible markup language (EXI) specifications, the documents size is minimized and authenticity still verifiable.

Using the suboptimal approach displayed in Figure 43, an XML document is signed and then broken up into fragments. The smaller fragment which is referred to as a partial document may contain critical information requiring a higher level of information assurance such as medical data, social security numbers and other such information that falls under the category of personally identifiable information (PII). The larger fragment may contain general information such that confidentiality is not that great of a concern. With the suboptimal implementation the last process prior to transmission with the partial document is compression. Compression on an encrypted document is expected to yield poor results. Using the example documents from the site http://www.web3d.org/x3d/content/examples/Basic/Security/index.html with the standard gzip tool on a MacBookPro and WinZIP on a Dell Precision M6400 both having block size of 4K each the following results are listed in Table 5.

		No Compression	WIN ZIP	GZIP	%WinZIP Compression	%GZIP Compression
HelloWorld.x3d		2133	906	814	57.5%	61.8%
Hello_WorldEncryptionInput.x3d		2710	1055	947	61.1%	65.1%
HelloWorldEncryptionResult.xml		5746	4481	4372	22.0%	23.9%
HellowWorldDecrypted.x3d		3816	1321	1219	65.4%	68.1%
HelloWorldSigned.x3d		6918	3173	3050	54.1%	55.9%

Table 5. Compression reduces the size of the file that conserves bandwidth. Between the two leading compression algorithm, GZIP and WinZip, GZIP is better. All compression algorithms used are lossless compression.

An EXI tool is currently under development at Naval Postgraduate School (NPS) Modeling Virtual Environment and Simulation (MOVES) Institue Scenario Authoring and Visualization for Advanced Graphical Environments (SAVAGE). Table 6 show results received from the current EXI tool. There are some variations between Table 5 nd Table 6, such as a 556 bit difference in file size of original HelloWorld.x3d.   This may be the result of an incomplete or unsuccessful download of an automated procedure of extracting the files from the Web site.   It is assumed that Snyder used the partial file for performing his analysis for the orignal x3d file. Variations in the size of the compression may be indicative to different settings used by different compression applications experiment. Regardless of the lossless compression algorithm used, the original file is always returned when decompressed.

	Helloworld	HelloworldDecrypted	HelloworldEncryptionInput	HelloWorldSigned
Original	1577	3816	2710	6918
GZIP	692	1195	917	3029
ZIP	836	1357	1091	3185
EXI NO (SCHEMA)	833	1162	1165	2989
EXI (SCHEMA)	523	737	735	2581

Table 6. A comparison of compression results using various lossless compression algorithms provides promising results for EXI integration.

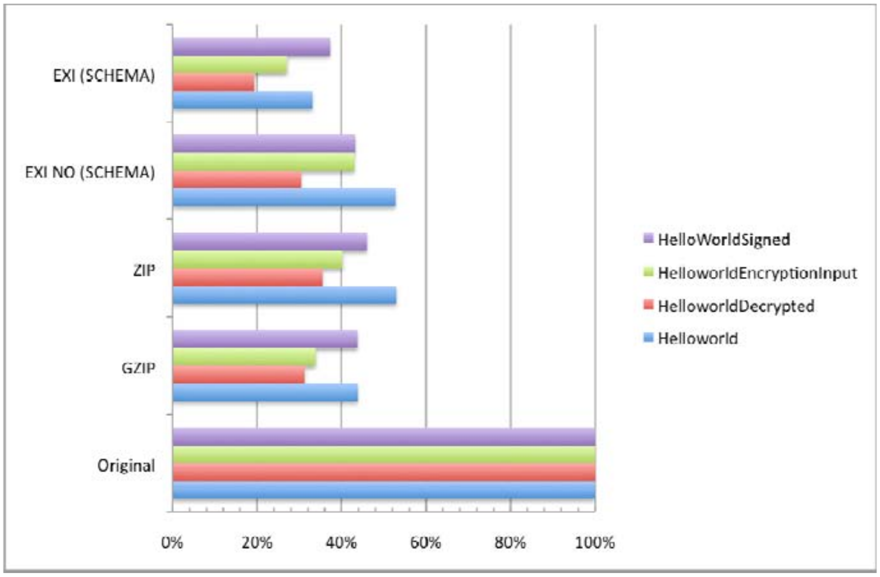


Figure 44. The shorter the line the greater the compression with this visual comparison of lossless compression performance between ZIP, GZIP, and EXI.

Encrypted files that are also compressed gain a slight size reduction without affecting the content because ASCII or Unicode representations of the encrypted data may use fewer bits per character generated. The lossless compression algorithm removes the slack resulting in a smaller file for the same data.

The issues that make Figure 43 suboptimal are that

- Partial XML file is not encrypted and therefore they are transmitted in the clear through the insecure transport. Therefore, confidentiality is degraded with this implementation.

- The entire document cannot benefit from EXI compression. Therefore, the document may be larger. Alternate compression algorithms can compress the encrypted data and thereby reclaim the unused bits used from character generation. Each character exists in one or more 4 bit blocks. If a character requires 6 bits then 2 blocks are used which means that 2 bits can be reclaimed by the compression algorithm. Therefore, the compression algorithm removes the slack prior to transmission of the encrypted file that gives approximately a twenty percent space savings.

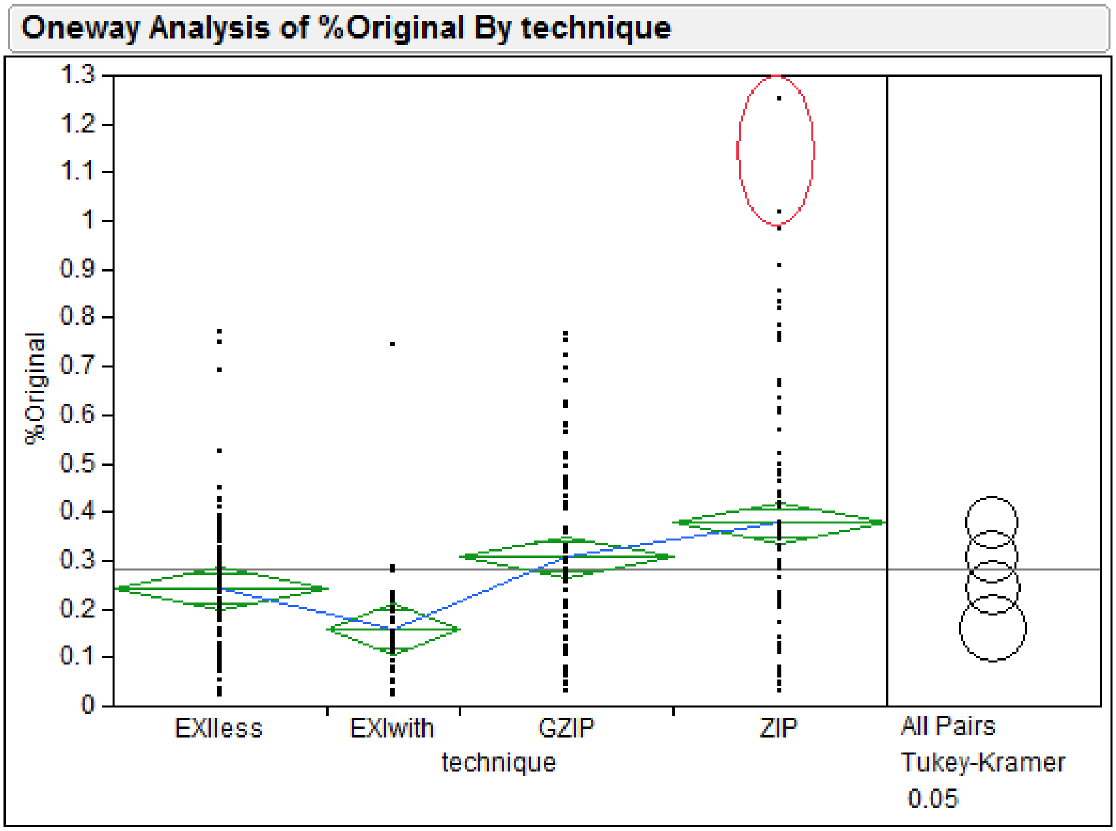
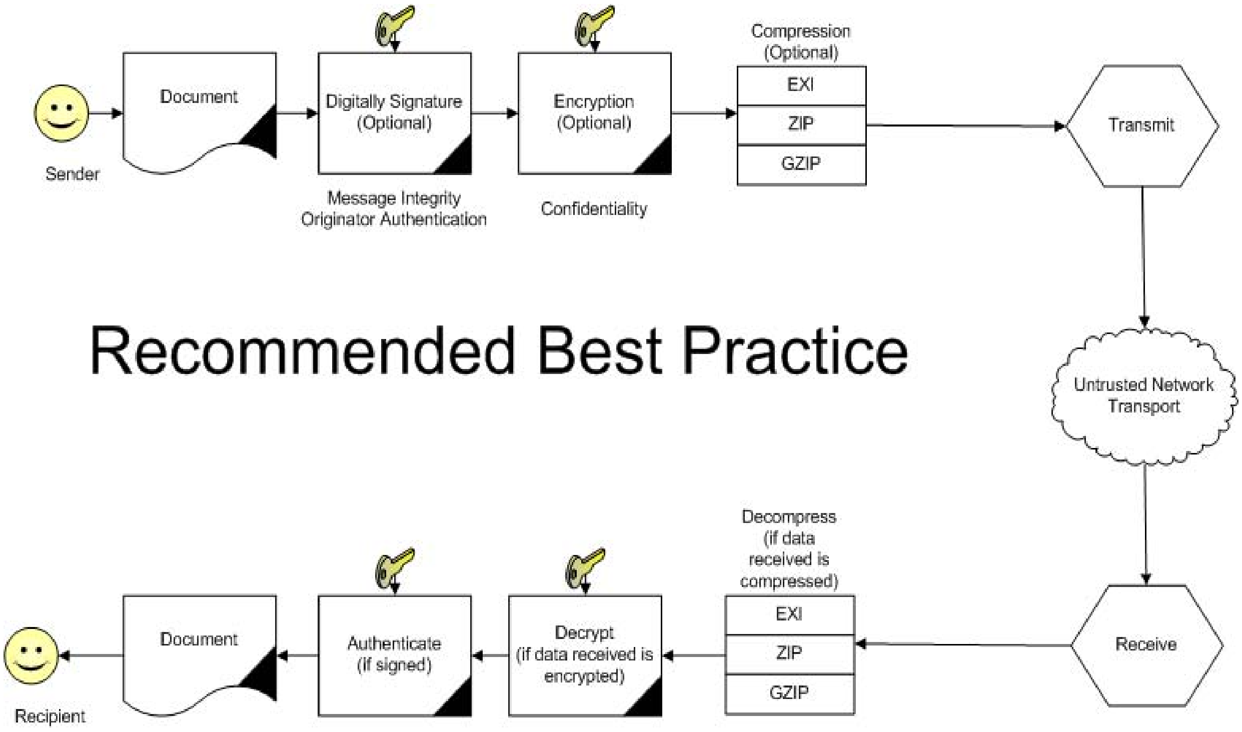


Figure 45. An ANOVA illustrating the effectiveness of the applying Efficient XML Interchange (EXI) compression over alternate forms of lossless compression algorithms represented in Table 6 (Snyder 2009).

Another approach to the implementation of XML signature, XML encryption and Compression is illustrated in Figure 46. Notice that in contrast to the suboptimal view the document is not split into multiple fragments. The end user determines which feature set is required to send the message or document through a seemingly insecure transport in efforts of achieving the desired levels of protection.


Sender
Document
Digitally Signature (Optional)
Message Integrity
Originator Authentication
Encryption (Optional)
Confidentiality
Compression (Optional)
EXI
ZIP
GZIP
Transmit
Recommended Best Practice
Untrusted Network Transport
Receive
Decompress (if data received is compressed)
EXI
ZIP
GZIP
Decrypt (if data received is encrypted)
Authenticate (if signed)
Document
Recipient

Note: Lossless compression algorithms exploit statistical redundancy, therefore, degradation in expected performance in terms of compression exist if data is encrypted prior to compression. All XML signed documents must use a lossless compression algorithm. A lossy compression algorithm will invalidate the digital signature. The savings when using a lossless compression algorithm comes in removing unused bits. ASCII may use 6 of 8 bits therefore there would be a savings of 2 bits per character.

Figure 46. This recommended approach to combining XML Signature, XML Encryption, and XML Encryption supports secure exchange of messages that require various degrees of security and compression.

In this manner, a document can be an XML digital signature can be applied to the document and the document can be compressed using EXI compression. It is important to note that EXI and XML Encryption only works with XML files. Therefore, XML compression is always performed after XML Encrytion. The benefits of this implementation are

- Security is at the discretion of the user. Based upon the message content the user may elect to neither digitally sign the document nor encrypt the document but send it as plaintext. Likewise, if the document is of a sensitive nature, the document can be encrypted digitally signed, and encrypted via XML and then compressed with an alternate lossless compression algorithm.

- More secure than suboptimal implementation. Since the approach illustrated in Figure 45 encrypts the entire document, it is more secure than splitting the document and sending part of it in the form of a multipart document in the clear.
- Full exploitation of XML EXI. If confidentiality is not an issue and the option is not selected, then the document can still support the security elements of message integrity and sender authenticity through the use of the digital signature. Thereafter, the digitally signed document can utilize EXI compression to achieve the best compression ratio available as illustrated in Table 6 and Figure 44.

The recommended goal for XML Encryption and Authentication is to have EXI as part of the XML result document. It is evident that there are various flavors of unclassified information. Each flavor can be categorized as requiring confidentiality, message integrity, or sender authenticity. Therefore, if the user is aware which is required or desired then it is possible for either a MAC or a DAC to be employed in relation to the subject matter. When using DAC, the end user enacts his or her criteria based upon message sensitivity to operation participants. The user's criteria are based upon practicality and organizational policy in regards to the use of XML digital signature, XML encyrption, and the compression method.

If Bob wanted to send Alice a message and Bob merely wanted to ensure that Alice knew the message was from him and that it had not been altered during transmission, Bob would select XML Digital Signature. Confidentiality was not Bob's concern. Now if Alice wanted to respond to the message and add personal information such as medical status then confidentiality becomes and issue and she would digitally sign and encrypt the message. Now that Bob has received the message he wants to forward pertinent portions of the document to the Charlie, a medical officer on board a bandwidth-constrained vessel. He removed the PII sections of the document and digitally signed the document. Bob then selects EXI compression to get the message to the smallest possible size for transmission. In this configuration Bob's goal was to satisfy authentication, message integrity and size reduction. However, successful organizations constantly evolve. Therefore, organizational policy must adapt to technological and social advances. Bob's organization has deemed that it must protect all organizational data transmission from being susceptible to data aggregation. This means that all information must be encrypted. The recommended goal for EXI integration with XML performs all of the formentioned tasks and is ready for a series of new evolutions in organizational policy.   Figure 47 illustrates the recommended goal in relation to how data can be securely passed between Bob and Alice within the constraints of practicality and organizational policy.

Unlike the optimal and recommended approaches this solution also supports multipart encryption. The W3C specifications for XML Encryption allows for the encryption of XML fragments such as credit card numbers, social security numbers, etc. This is a common practice for secure Web enabled information exchange. With technologies such as SOAP and SAML, the Web-based security mechanism assists in developing solutions. However, message and document-centric security involves placing security at the document level without the reliance of external factors. Once the document is received, the information revealed is completely dependant upon the recipient's credentials. Web-based security mechanisms can augment message and document-centric security by supplying a secure venue in which user rights can be elevated based upon need or urgency of the data. Naturally, this would require two-factor authentication that is satisfied by the existing user's certification (if valid) and something unique to that individual or entity (biometrics, password, physical cryptographic insertion key, etc.). XML Fragments are contained within XML documents.

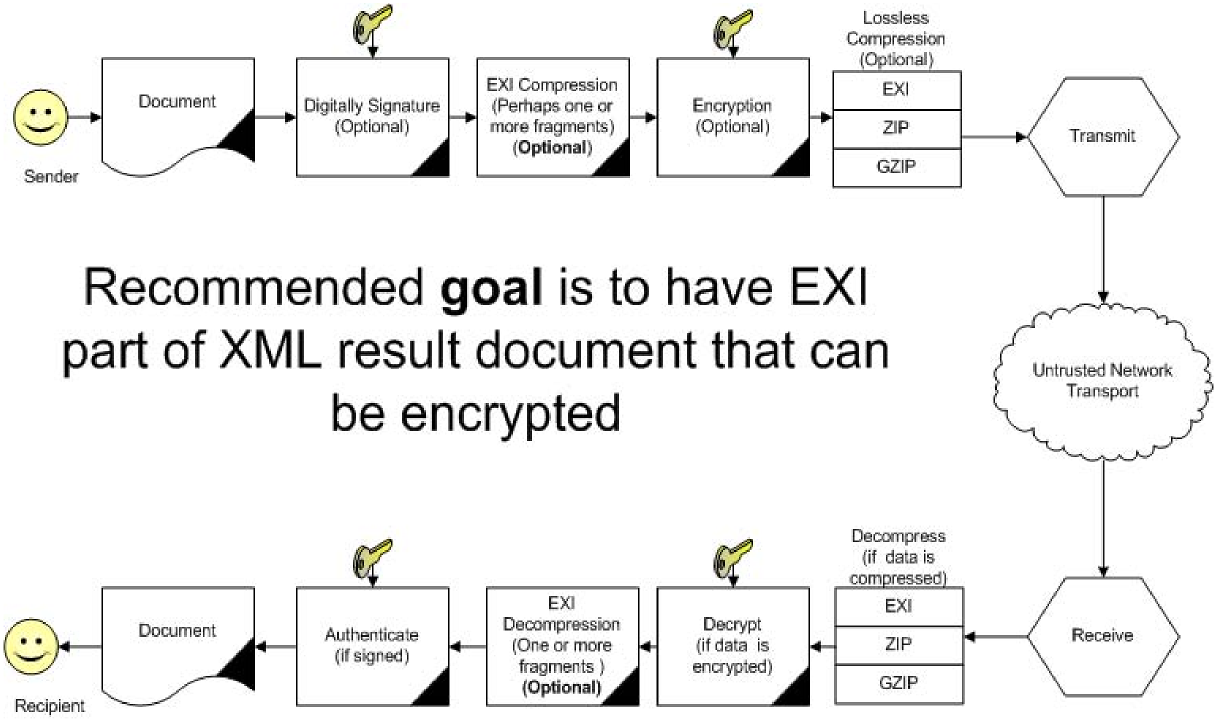

Sender
Document
Digitally Signature (Optional)
EXI Compression (Perhaps one or more fragments) (Optional)
Encryption (Optional)
Lossless Compression (Optional)
EXI
ZIP
GZIP
Transmit
Recommended goal is to have EXI part of XML result document that can be encrypted
Untrusted Network Transport
Receive
Decompress (if data is compressed)
EXI
ZIP
GZIP
Decrypt (if data is encrypted)
EXI Decompression (One or more fragments) (Optional)
Authenticate (if signed)
Document
Recipient

Figure 47. Incorporation of the EXI compression algorithm as a native part of XML document yields the benefit of maximum compression with secure communications.

D. TEST CORPUS OF EXAMPLES

1. Everyday Steaming

Each day deployed or underway there is a requirement for to share messages amongst participating partners. These messages may be as simple as the unit situation reports to operation reports with high order of precedence.

In Admiral Gary Roughhead’s address to the Navy League Sea, Air, Space Banquet dtd May 5, 2009, he stated “People look quickly at our Navy and think My, those ships are so incredibly powerful, and there seem to be so many of them. The do not always consider that the 283 ships that serve in our Navy today are the fewest that we’ve had in our fleet since 1916 … The fleet must cover Americas responsibilities around the world, 24-hours a day, seven days a week and at an unforgiving pace of operations. The security of the oceans is an assumed constant, and so the security is forgotten at least until there is a significant or newsworthy interruption like the attempted pirating of the Maersk Alabama … We require unimpeded use of the sea and the global commons to conduct 90 percent of our trade…"

Two-hundred and eighty-three ships U.S. flagged ships is excessively thin to meet U.S. national interests world wide without multinational/multiagency participants such that a mutually beneficial relationship can be formed. Piracy is one of issue that affects all nations who export to other nations by sea. If allowed to go unchecked, several nations may loose a large percentage of their gross national revenue that may cause further global economic instability and marked increase in the unemployed populace. To combat this issue several agencies and nations are operating within the same theatre of operations in a collaborative effort to eradicate piracy from the high seas. Unfortunately, incompatibilities between communications systems still exist that may result in delays in pursuing and/or capturing vessels suspected of harboring, abetting, or engaging in acts of piracy.

A typical day for units engaged in antipiracy operations may begin at 0000 with a standard checkin such that all units within the taskgroup report in. This is normally performed via voice channels but can be supplemented via XMPP chat for Web enabled entities. A Web enabled session supplements voice by adding a level of clarity and reducing man-made errors that may be made when copying instructions within the official log book. All agents involved not only hear but also see the instructions or confirmation as they are relayed over the air. Prescheduled check-ins are common to all operations especially those involving multiple partners such that the operational commander is accountable for each entity under his charge. Figures 48 and 49 show the typical check-in process of the commands underway where HZ is the sea surface commander requesting participating partners to respond to its initial communiqué. Any ship that fails to respond is queried again to discover the commands communication malfunction: equipment, lack of attention to detail, out of transmission range, etc. In some cases the unit may be out of transmission range but may still be accessible via the XMPP chat session.

```
HZ:   All units in Romeo Tango Papa this is Hotel Zulu, over
Ship 1: This is Golf Papa Papa, Roger Out
Ship 2: This is Uniform Quebec Charlie, Roger Out
Ship 3: This is Oscar Mike Echo, Roger Out
HZ: This is Romeo Tango Papa, Roger Out.
```

Figure 48. Text representation of a check-in process.

```
<MSGLOG>
        <Originator>
                <DTG>2008-10-20T00:00:02.0000000+02:00</DTG>
<CallSign>HZ</CallSign>
<Message>All units in RTP DE HZ over </Message>
</Origator>
<Response>
<DTG>2008-10-20T00:00:45.00534200+02:00</DTG>
<CallSign>GPP</CallSign>
<Message>DE GPP RGR OUT</Message>
</Response>
<Response>
<DTG>2008-10-20T00:01:28.3523210+02:00</DTG>
        <CallSign>UQC</CallSign>
<Message>DE UQC RGR OUT</Message>
</Response>
<Response>
<DTG>2008-10-20T00:03:35.04321435+02:00</DTG>
        <CallSign>OME</CallSign>
        <Message>DE OME RGR OUT</Message>
</Response>
        <Originator>
                <DTG>2008-10-20T00:00:02.0000000+02:00</DTG>
<CallSign>HZ</CallSign>
```

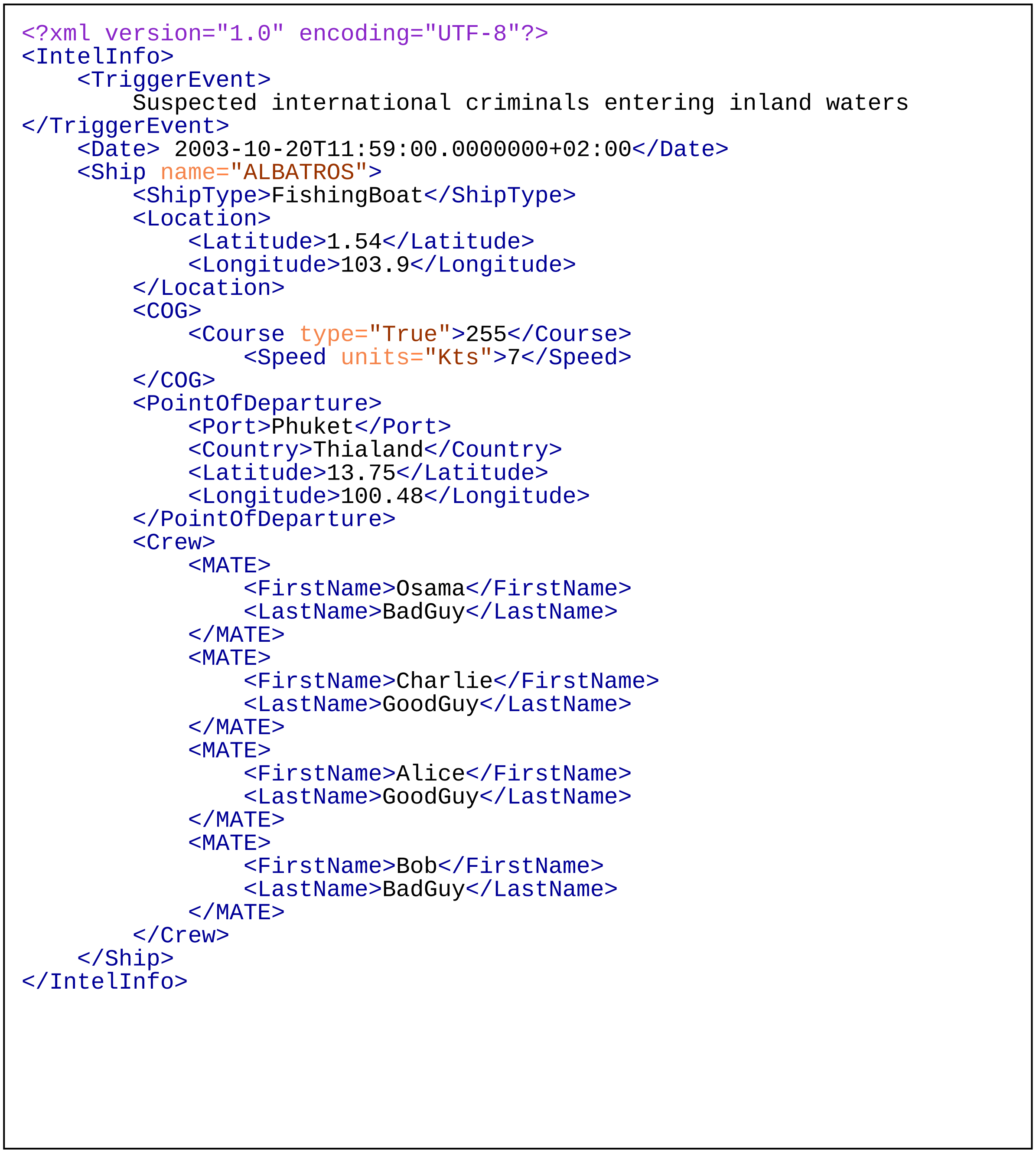
Figure 49. An example of a possible XML representation of the Daily Check-in Underway is presented. All information is structured, which facilitates parsing of information.

Figure 49 illustrates a potential XML-based log of the daily check-in interaction between all commands in company. This log is useful in performing a cross comparison of network connectivity and associated hardware, software, user training issues because XML data can be parsed and it can be determined who failed to respond which is validated by the corresponding entity’s daily status report.

2. Secure Information Exchange

Controlled Unclassified Information (CUI) may need to be exchanged between agencies of different nationalities. If a vessel is being tracked off the coast with a passenger manifest that contains the name of possible wanted criminals by another nation, then the Intelligence agencies may desire to exchange information with each other without exposing their national databases. As the information ship’s track is in constant motion, both agencies know that the information is perishable. Therefore, time is a major priority as the ship leaves international waters and enters Singapore inland waters. The intelligence agent quickly establishes contact with the Singaporean harbor patrol and sends them a digitally signed encrypted message using XML security.

The agent’s message does not reveal the source of the information but because it is digitally signed and a trust relationship has been established between the two nations department of homeland defense, they were able to take action. Figure 50 illustrates a possible XML file prior to signing and encrypting the file. It reveals pertinent information about the location of the vessel and the fact that it has both neutral and hostile entities onboard. With this information the Singaporean harbor patrol can determine what kind of force is required to support the arrest of the individuals.



```xml
<?xml version="1.0" encoding="UTF-8"?>
<IntelInfo>
    <TriggerEvent>
        Suspected international criminals entering inland waters
</TriggerEvent>
    <Date> 2003-10-20T11:59:00.0000000+02:00</Date>
    <Ship name="ALBATROS">
        <ShipType>FishingBoat</ShipType>
        <Location>
            <Latitude>1.54</Latitude>
            <Longitude>103.9</Longitude>
        </Location>
        <COG>
            <Course type="True">255</Course>
                <Speed units="Kts">7</Speed>
        </COG>
        <PointOfDeparture>
            <Port>Phuket</Port>
            <Country>Thialand</Country>
            <Latitude>13.75</Latitude>
            <Longitude>100.48</Longitude>
        </PointOfDeparture>
        <Crew>
            <MATE>
                <FirstName>Osama</FirstName>
                <LastName>BadGuy</LastName>
            </MATE>
            <MATE>
                <FirstName>Charlie</FirstName>
                <LastName>GoodGuy</LastName>
            </MATE>
            <MATE>
                <FirstName>Alice</FirstName>
                <LastName>GoodGuy</LastName>
            </MATE>
            <MATE>
                <FirstName>Bob</FirstName>
                <LastName>BadGuy</LastName>
            </MATE>
        </Crew>
    </Ship>
</IntelInfo>
```

Figure 50. Structured information can be passed from agent to authorities in a secure fashion. Intelligence data exchanged between nations adds value to mission planning.

3. External Communication with Multinational and Multiagency Partners

In years past, one would correctly assume that the flagship to which the report would be made is of U.S. origin for a U.S. task force. This is an obsolete frame of thought. While loyalties rest with their own country, actual operations in the world of today and that of tomorrow are being conducted with multinational and multiagency forces. Some are formed out of necessity in which prior planning was not possible. Nonetheless, there exists the requirement to securely transmit information of a sensitive nature while maintaining records beyond that of a bridge-to-bridge conversation. To this end a standards based approach must be employed to ensure that units capable of receiving data/information via the radio frequency spectrum can use their own tools, negotiate the appropriate cryptographic algorithm to use, and implement secure data transfer between and amongst partner nations.

As the day develops, a ship with a multinational crew within the coalition that utilizes Autonomous Vehicle Control Language (AVCL) wants to send track information to another ship that uses Keyhole markup language (KML), such that the reports can be generated from the unmanned aerial vehicle to facilitate the commanders daily intentions. The unmanned areal vehicle examined the area of interest in which a possible hostile entity operating off the coast of Eritea was weighed anchor off the blind side of one of the islands. The formats are incompatible. However, they can be adapted to use the other via XSLT. The XSLT adapt to the new format based upon the published schema to translate position information to a format that the other ship understands. An XSLT was also used to adapt raw AVCL data to KML as can be seen in appendix C. An operator initates the request from the ship's data repository. The process is illustrated in Figure 50 Appendix C contains a sample XLST and it's associated data output file. At the time of this writing, the name of the NPS SAVAGE repository is called TrackDataConversionHub.

Once the file is received, its origin is verified as well as the base requirement for well-formed XML. It must be well-formed and valid XML to be processed properly. The document validates the recipient's creditials as an authorized user and decrypts any

XML elements that have been encrypted for a select group. This factor is important when transmitting sensitive data to a multiagency and multinational organizations. There may be proprietary data that is not releasable to certain countries or information that may contain not releasable to foreign entities (NOFORN). The capability is important for tactical situation as layed out in the Secretary of the Navy Instruction 5510.36, Information Security Program. Other nations and other entities also have their restrictions in relation to releasability of information. In operations, knowledge is key and XML Encryption and authentication is an enabler.

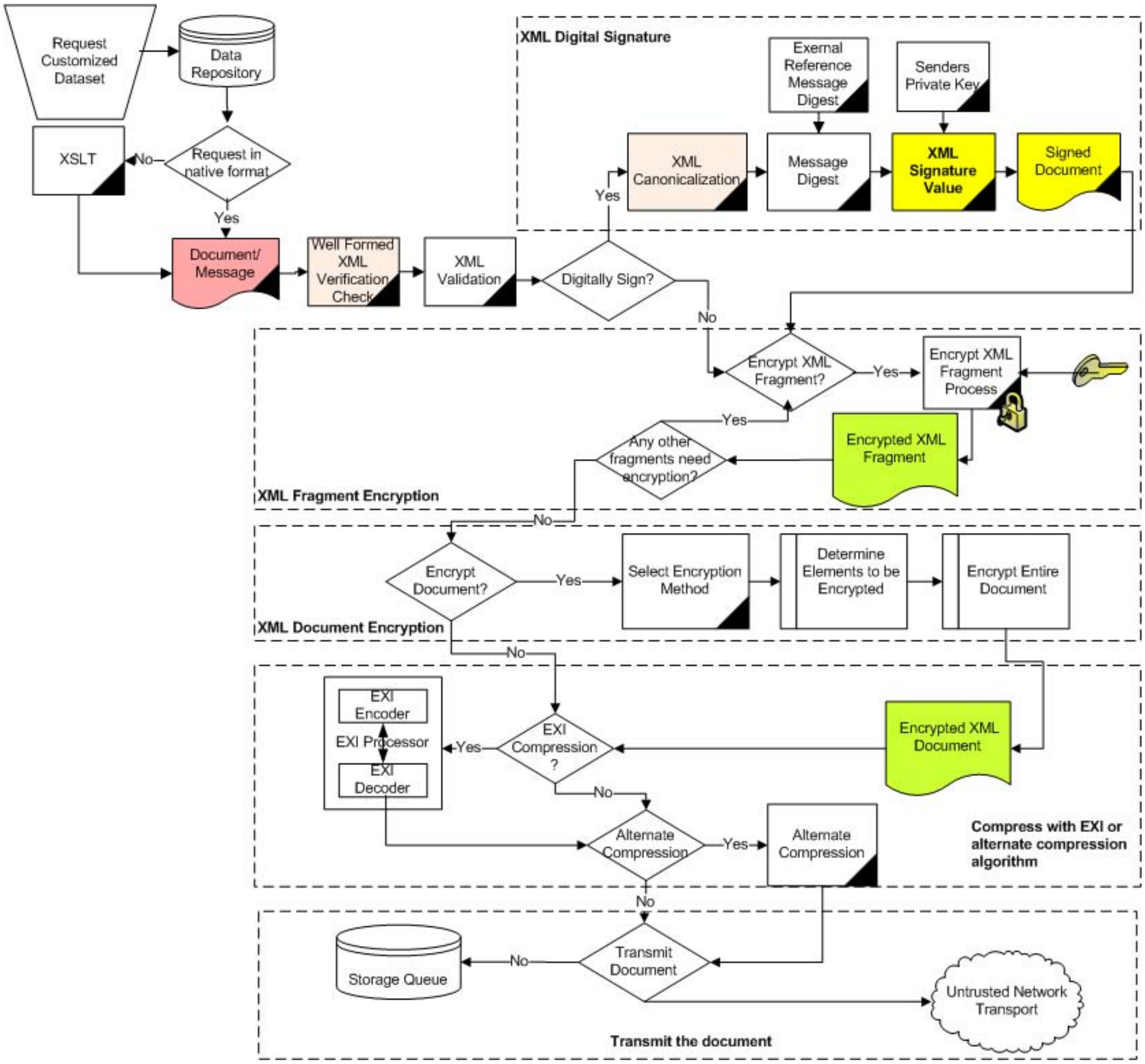
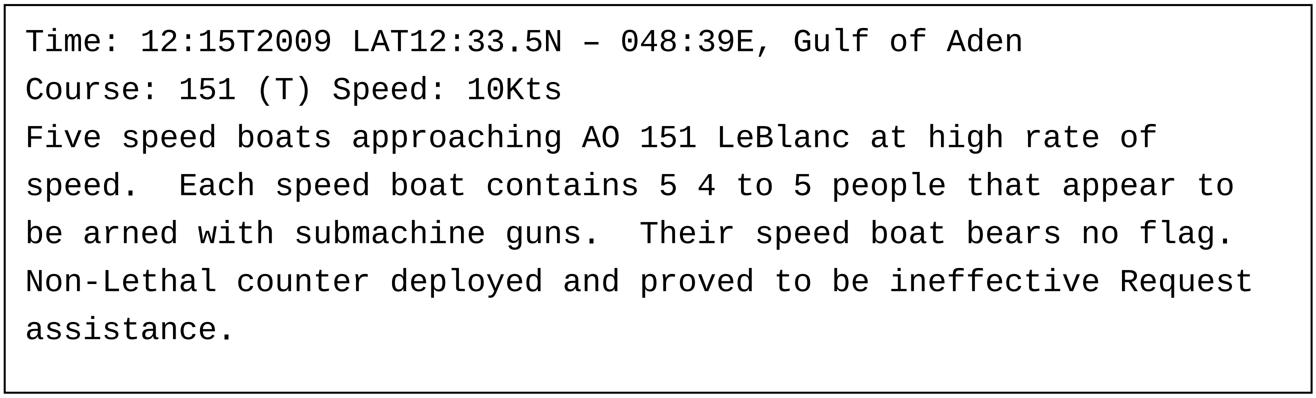


Figure 51.   One approach to applying XML security is displayed such that the originator chooses which facet of security is important, and assign it to the message accordingly.

Throughout the day, the task force exchange messages relating to possible tracks. Those messages are sent to each unit’s data repository and correlated such that tracks are updated. It is one of the method of conducting over-the-horizon operations (OTH) which in a nutshell is simply extending the range of own ships capability by correlating data from other assets to form a common operating picture (COP). XML encryption and authentication is primary candidate to ensure interoperability between coaltion and multinagency partners.

At 1218 radio, the battle watch captian (BWC) receives a transmission from a pleasure craft. The message is not encrypted; however, it is digitally signed. The message simply reads as illustrated in Figure 52. Although XML is readable, it is not meant to be read in the raw. The output to the display is formatted such that it is more palatable to read. XML is meant to be parsed by machines or programs to extract the information required on demand. Figure 53 illustrates a possible representation of the XML file once its fully processed by a cascading stylesheet (CSS).



```
Time: 12:15T2009 LAT12:33.5N – 048:39E, Gulf of Aden
Course: 151 (T) Speed: 10Kts
Five speed boats approaching AO 151 LeBlanc at high rate of
speed.  Each speed boat contains 5 4 to 5 people that appear to
be arned with submachine guns.  Their speed boat bears no flag.
Non-Lethal counter deployed and proved to be ineffective Request
assistance.
```

Figure 52. XML is readable, but it is not meant to be read. It is meant to be parsed and processed into a more user friendly form. This is a possible representation of one form in which an XML file can be represented to the user.

The raw XML file is illustrated in Figure 53. It is structured such that pertinent data can be parsed and transmitted to a host of other entities. If a military unit had an unmanned aerial vehicle (UAV) operating in the area, then it is likely that it would send it position and interecept course information based upon projected speed over ground Latitude and Longitude to revector to the current threat position. With this information, the UAV arrives in the area and streams video back to the combatant vessel to properly appraise the situation. The commander can then devise a more cohesive plan to take a proper and preferably non-violent course of action but is always ready to be prepared to return fire if warranted.

The UAV arrives on station and begins streaming video back to its operator. The operations specialist (OS) projects that the speedboat may overtake the Leblanc within 10 minutes. They also calculate own ships capability and other ships operating within the given area, if speed is increased to ahead flank. Bottom line is that within the constraints of time, the pirates may achieve their goal of boarding and possibly taking over the ship unless another entity can intervene.

A French flagged patrol craft that is operating in the area is alerted to the situation and reports that it can be there within the allotted time. All data is passed to the French operations officer via voice and secured e-mail implementing XML security. The message the French received resembled that in Figure 53. The French system translated the message to their format and possibly to their native tongue after verifying the message authenticity and message integrity. The French patrol craft take action and cause the pirates to abandon their chase. However, due to the French policy the vessel is not boarded but the French issue Level I and II queries demanding their intentions and requesting that they stop or be fired upon. They are successful in detaining the suspected pirates until the international vessel arrives on station that is equipped with the appropriate equipment to take the vessels in addition to have the appropriate personnel onboard to legal detain the pirate suspects.

```
<Message>
     <From>
          <HullType>AO</HullType>
          <HullNo>151</HullNo>
          <UnitName>Leblanc</UnitName>
     </From>
     <To>
          <GlobalEmer>ALL SHIPS IN TRANSMISSION RANGE </GlobalEmer>
     </To>
     <Subj> SOS – ATTACK IN PROGRESS </Subj>
     <Date>05292009T12:15:34</Date>
     <Position>
          <Latitude orientation=”N”>12:33.5</Latitude>
          <Longitude orientation=”E”>048:39</Longitude>
          <Name>Gulf of Aden</Name>
     </Position>
     <Course reference=”Magnetic”>151</Course>
<Speed>10kts</Speed>
     <FreeText>
Five speed boats approaching AO 151 LeBlanc at high rate of speed.
Each speed boat contains 5 4 to 5 people that appear to be arned
with submachine guns.  Their speed boat bears no flag. Non-Lethal
counter deployed and proved to be ineffective Request assistance.
     </FreeText>
</Message>
```

Figure 53. XML is structured data that although human readable is not meant to be read. It is meant to be processed. The above is an XML message received from the notional Canadian flagged oiler LEBLANC AO 151. Pertinent data exists within tags that can rapidly be parsed and sent to another entity.

The commander’s vessel is estimated to take at least 16 minutes to reach the area. However, another vessel of similar capabilities is closer to the area and can be there within 8 minutes at its maximum speed. Notionally, all entities that send and receive transmissions have some method of encrypting their communications channel. However, in reality there exist vessels that lack that capability. Therefore, if confidentiality is not an issue a message or document would simply bear the digital signature. Using Figure 44, a trace of such a message can be performed. The end result would yield message integrity and sender authentication.

4. Document and Message Disemination

As the day progresses, several other messages are generated and transmitted. With each message transmitted and received, the concern is focused on one of three areas: Confidentiality, Integrity, and Authenticity (CIA). Each message transmitted and received has a specific level of assurance that must be maintained. Additionally, most messages require some sort of action on the part of the recipient. That response may be as simple as an acknowledgement of receipt such that the sender has assurance of delivery. Alternately, the response may mandate specific and deliberate action on the part of the recipient such as required upon receipt of an operation order (OPORD), which may direct a ship to support a specific humanitarian assistance disaster relief request of in support of another nation or group.

XML digital signature and encryption techniques assist in achieving a high level of assurance by securing one or more areas within the scope of CIA. CIA is ensures that the message maintains information in such a manner that only the intended individual may be able to view it. Additionally, it ensures that the message has not been altered in any way. Table 7 illustrates what is gained by XML digital signature and XML Encryption.

	Non-Repudiation	Authenticity	Confidentiality	Integrity
XML Signature	X	X		X
XML Encryption			X	

Table 7. XML Signature and XML Encryption fits neatly into one of four different categories. Table 7 shows which category each action satisfies within Authentication, Confidentiality, Integrity and Non-Repudiation.

There are times when no security is required as in the event of a "Save Our Ship" (S.O.S.) message (USCG 2003). It would be nice for a message to come digitally signed but upon receipt, all units within the vicinity must respond until the affected entity is safe and secure. This is the one of the several laws of the sea as established by UNCLOS. Whenever a distress message is received, response time is critical. All ships that receive the message are are in the vicinity hasten to the reported area to render assistance. Table 8 illustrates a list of other document types that require a specific level of security to meet the Information Assurance (IA) requirements.

	Non-Repudiation	Authenticity	Confidentiality	Integrity
Non-Official General E-mail	X	X	X	
Official E-mail	X	X	X	X
Message Traffic	X	X	X	X
Track Data	X	X		X
Military Track Data		X	X	X
Position Report	X	X	X	X
General Public Distribution		X		X
General Online Gaming		X		X
Financial Transaction	X	X	X	X
Save our Ship				
Blog Site		X		X
Operation Report	X	X	X	X
Situation Report	X	X	X	X
Daily intentions Message	X	X	X	X
Equipment Status Report	X	X	X	X
Standard Automated Logistics Toolset (SALTS)	X	X		X
Communications Report	X	X	X	X
Public Affairs Officer News Release	X	X		X
General Digital Imagery		X	X	X
Geospatial Satelite Position Reports		X		X
Global Position Report Updates		X	X	X
Military Massive Multiplayer Online Game		X	X	X

Table 8. All data can be classified as requiring attributes to achieve confidentiality, authentication, integrity, non-repudiation or none of aforementioned.

E. SUMMARY

XML digital signature, XML encryption, and efficient XML compression can be used for a host of different operations. It is adaptable and ready for changes in organization policy. Without EXI compression, a modest savings in bandwidth can be achieved. However, with the full implementation of EXI a more robost infrastructure can be formed that is friendly to bandwidth-constrained entities. Security and practicality combine with the implementation of DAC such that dynamic decisions can be made to support current and future operations. This enables unclassified information to flow between systems having dissimilar architectures support some or all of the W3C XML recommendations. A privately owned pleasure craft may have no need to forward encrypted data but supports XML digital signature and authentication.

IA requirements vary with the message type and document content. XML security is ready for the changing roles by enveloping and encrypting message fragments to support transactions. As society continues to migrate to the information age, encryption becomes a more pressing issue. States such as Nevada and Massachusetts have already taken measures to protect its citizens with Nevada's NRS Electronic Transmission Lay 597-970 and Massachuesetts 201 CMR 17 (NRS 2008) (CMR 2009). Other states and other nations may soon join the fray and XML security can be considered as a prime contender for an international standard.

Message and document-centric security is task appropriate for multinational and multiagency operations. The concepts of XML Digital Signature, Encryption, and XML compression can be used with XMPP chat, any message and any document.

VI. EXEMPLAR CASE STUDY APPLICATION OF TECHNOLOGIES

A. INTRODUCTION

To achieve national interests, maritime leaders seek a commonality to engage in operations jointly. This bond facilitated the establishment of CTF 151 and NATO ATALANTA in support of operations throughout the Gulf of Aden/Horn of Africa. All operations inclusive of dynamic operations require a degree of planning else nations may not be able to securely communicate with one another. The communications requirement involves ensuring cryptographic algorithms and processes are readily available to current and future participants within a dynamic networked environment to include foresight as to the value of the information and an estimate of time to decrypt information passed via illicit means. However, even if carefully planned, equipment failure generally occurs at inopportune times, therefore, a task force requires the ability to act exchange information with pertinent participants inclusive of reports of unfortuneate events. XML Security can help, but there does not exist a technology devoid of vulnerabilities. Vulnerabilities must be considered to develop tactics, techniques, and procedures to mitigate their effect on operations.

B. ENVIRONMENT

Ensuring the sea lines of communications to ensure safe passage of commercial shipping through international waters is considered the topmost priority. As much of the world’s commerce is conducted by sea, this exacerbates the issue of piracy such that they are not just a nuisance but a threat to the economic health of all seafaring nations.

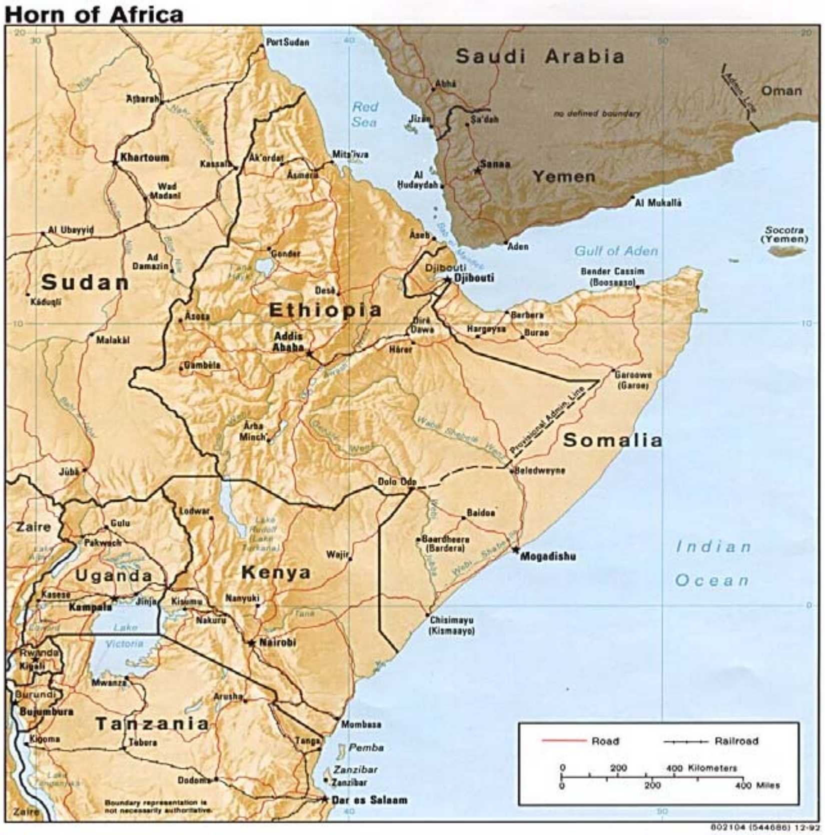


Figure 54. The area of responsibility (AOR) for CTF 151 and ATALNATA is the Gulf of Aden/Horn of Africa (Reliefweb, Office for the Coordination of Humanitarian Affairs 2009).

The motivation of this set of exemplars focus on the use of document and message centric XML security in passing and receiving messages to and from coalition partners on an average day during a coalition task force. CTF 151 Operation Allied Protector, Operation Ocean Shield and Nato's Operation Atalnata have converged on the Gulf of Aden, Horn of Africa to support maintaining the lines of communications to all commercial shipping. NATO has even established a dedicated password protected Web site to get the word out to units operating in the area and created a Web site http://www.mschoa.org, to get the word out to as many as may register for the site.

1. Preparation for Operations

Due to the dangerous nature of the sea, a vast amount of preparations are required to transit across the open ocean. Seafarers follow the seven Ps to ensure their preparadness for the inherent dangers of their trade. The seven Ps are Proper Prior Planning Prevents Pretty Poor Performance. Therefore, preparations must be made for every evolution that the ship may encounter. The overarching communications plan is known as the Operational Tasking Communications (OPTASK COMMS). The requirement to have an OPTASK COMMS does not change from any other normal underway function.   Satellite access request for INMARSAT, EHF, and HF frequencies are still required. Additionally, as seafarers transit from point to point the authorized frequency for the local region may be change. The communications or radio officer is responsible for putting the plan together and coordinating with domestic and multinational organizations to obtain the appropriate frequencies. An example OPTASK COMMS message is in Appendix A.   The difficult part in drafting the OPTASK COMMS is discovering both the communications capabilities and each unit's requisite status when drafting the plan. In the past, the cryptographic requirements were worked out prior to departure or might be sent via over-the-air-transmission (OTAT) to capable units. However, that is with a homogenous task force. Today's mission heterogeneous force structure is more spontaneous than ever before. More nations see piracy as a threat to the sea lines of communications and can no longer consider it a public nuisance. It has an indirect affect on the nation's economic health especially for those nations that depend upon the sea for export and imports of their goods.   For such nations in which their period of participation is brief, Message and Document Centric XML Security is most appropriate for exchanging information securely. Assume that a Chinese flagged vessel desires the protection of the OP ATALANTA or CTF 151 while it conducts a night transit through the straits of Aden/Horn of Africa. It is unarmed but has e-mail and basic Web browsing via commercial Super High Frequency (SHF) Satellite Communication (SATCOM) Internet e-mail exchange cloud computing based service onboard. The support facility ashore receives the e-mail and forwards to the battle watch captain onboard the flag ship. Meanwhile, there is a fishing vessel conducting operations and covertly gathering intelligence. It is between the Chinese vessel and the flagship. On the surface, the vessel slowly trawls the ocean with the ball-diamond-ball configuration on its flagpost, which means that it is restricted in its ability to maneuver. The Battle Watch

Captain (BWC) of the North Atlantic Treaty Organization (NATO) force forwards the Chinese vessel's master his identity encrypted with his corresponding public key. The Chinese vessel's master returns the nonce and adds one of its own along with its identity encrypted with its public key. At this point both parties know that they can securely communicate with the other and the last response would be that the BWC forward the schedule of transit rendezvous times digitally signed and encrypted with the other's public key and their corresponding nonce. In the meantime, the pirate's agent continuously monitors the RF spectrum and intercepts what appears to be a garbled message. The vessel continues to collect transmission in hopes of collecting enough packets to swiftly discover the initialization vector and eventually the key to break current and future messages.

Unfortunately for the intelligence collection vessel, the vessels have already authenticated to each other and are using message and document centric security. The units can securely exchange data with a high degree of assurance using document and message centric security and other protocols to encapsulate and further protect the message the message. The strength of the encryption is dependent upon the algorithm in use and the key length; therefore, both the algorithm and key length is based upon the value that the organization places on the information.   For example, if the organization decided to use data encryption standard (DES) which is weaker than triple data encryption standard (3DES) for information that may be deemed to be of high national interests but not yet satisfy the requirements for more stringent safeguards then the estimated time to break the encoding can be achieved by an entity of modest technical ability. By the time the encryption keys are broken, the knowledge is stale and therefore useless to the pirate collection vessel. Currently advanced encryption standard (AES) is the National Security Agency (NSA) approved and recommended algorithm for the United States government. As of this writing, there are no international laws against passively scanning and collecting of packets. However, several domestic laws within the United States prohibit such action. For example, the state of Nevada Senate Bill Number 125 Section 1 Chapter 205 prohibits the capture, storage, or reading of information from the radio frequency identification document of another person without the other person's knowledge and **prior** consent for the purpose of committing an illegal act. Piracy by definition is an illegal act (Nevada Represented in Senate and Assembly).

The escort commander wants to forward information such that everyone knows what the plan by using the X3D-Edit tool to generate a visual representation of the plan such that each civilian ship in company can visually see and make preparations for the transit through pirate infested waters. The plan indicates the rendezvous, the standard distance that each ship must maintain from the other, the transit path, the turn around point, preplanned responses to pirate attack, and brevity code words to be used over bridge to bridge. It also mentions that a P-3 is scheduled to periodically patrol the airspace to further ensure that the path is clear of unnecessary threats. The information is compressed, digitally signed and encrypted using XML security. From this point all future messages are short and poignant. The system by which messages and documents are passed is e-mail because commercial vessels may not have requisite communications equipment aboard. However, each ship is required to download and install or use their own implementation of the World Wide Web standard for XML Encryption and Authentication.

If keys are not periodically changed, the pirate agent may eventually be able to crack or compromise the encryption key and decipher previous and future messages without being privy to either the secret key or digital signature.

Using the established encryption keys, the message is relayed to all ships scheduled to participate in the convoy. The message requests all units send a communications and engineering status report as well as their maximum achievable speed. The information is factored into the line up such that the slowest ship takes the lead position. A graphical representation of the procession is posted to a protected site such that each unit can download the X3D encoded data to their C4I suite and review offline as applicable. Naval Aviation Command has directed that flight crews be deployed in a standby posture in efforts of extending flight crew on station via reduction of hours in flight. Therefore, P3s and other assets are used to extend the OTH view of combatant vessels engaged in convoy duty.

The appointed hour approaches and all participants are required to check in with the lead convoy ship. The convoy ship performs a series of communications checks both voice as well as data. Secure XMPP chat channels are also verified with those units that are capable of performing chat. Each ship is directed to forward an XML message to the lead ship to verify their reported transmission capability is functioning properly. Upon completion of communications checks the lead ship issues a single order to all ships operating under the banner of HOA. The message “HOA DE HZ STANDBY TO EXECUTE PERSIAN SPEAR, OVER”. This is understood by all ships to mean “All participating units in operating in the Horn of Africa transit, standy to perform the transit. Please acknowledge receipt of this message. Upon receipt of acknowledgement from all participants , the order is given to begin as planned.” The ships respond “DE [CALL SIGN], RGR OUT.” Once all ships are accounted for the lead ship releases the statement “DE HZ, EXECUTE PERSIAN SPEAR, AR M SPEED 10 M CORPEN 250, OUT”. To reduce the language barrier between civilian and military shipping, XMPP chat channels used employ standard terminology with the civilian merchants that clearly spell out the message intent. The message the operators relay over chat simply state the following “This is the officer in charge of the convoy, please proceed in the prescribed order as planned. My course is 250 True and my speed is 10 Kts.” The military forces escorting the merchants are well aware that although brevity is preferred, it is meaningless to if the ships in company cannot understand what is being relayed, therefore, a general translation XSLT was available to all participants prior to the start of the event. The XSLT converted the standard terminology used with the brevity codes to the more civilian friendly equivalent. Military unit would have no need for the XSLT as all language used is within the scope of their standard voculary.

An hour into the transit, a P3 reports a small vessel dead in the water along the track which the convoy is taking. After failed attempts to bring the vessel up on bridge to bridge radio, the lead ship’s navigation team projects the time to intercept and assumes the vessel is non-hostile. However, erring on the side of caution new coordinates are transmitted to ships in company to avoid the contact-of-interest (COI) by 8000 yards.

Additionally, a message is sent to the country who has jurisdiction over the maritime region that the vessel occupies to investigate it further.

2. Casualty Reported

Communications checks proceed at regular intervals of 60 minutes to ensure all participants are on track are proceeding without incident as planned. During the transit, a situation report (SITREP) comes in from one of the merchant vessels stating that it has a casualty in the number 2 generator and is now degraded. The convoy is slowed to 7 kts in response to the added information. HZ dispatches a technician to the affected vessel to assist in repairs as the convoy continues to transit the Straits of Hormuz. Upon arrival onboard, the dispatched specialist reviews the damaged part and notes that there are no spares onboard. The dispatched specialist requests the unit's machine shop to restore the component to a serviceable condition. The estimated time of the repair is 2 hours. The technician returns to his ship, delivers the part to the machinist who completes repairs 30 minutes ahead of estimated time. The technician returns to the affected unit, reinstalls the part, observes the component working properly and returns to the HZ. HZ thereafter issues the command to increase speed to 15 kts to make up for lost time. Within hours, the transit is complete and all units at dispersed. HZ's commander releases a farewell e-mail to all ships within participating units, as it travels to the next rallying point to meet up with the convoy for the return voyage.

3. Aftermath of a Pirate Attack

Enroute to the rallying point, a message regarding the vessel that was dead in the water is received. MV MEARSKE ALASKA "ALL SOULS LOST TO SMALL WEAPONS GUN FIRE" was the bottom line of this message. The MV MEARSKE ALASKA was reported missing a week ago shortly after refusing to await a convoy to facilitate the transit with the comment that it would take them too far off schedule. The XML-based message and response were maintained at central headquarters as well as onboard the MV MEARSKE ALASKA. Evidently, they attempted to send out an S.O.S. message but according to the ships master's log, a rocket-propelled granade (RPG) destroyed their transmitting antenna prior to them getting the opportunity to successfully send out a message.   Surviellance recovered indicates that the pirates became enraged when one of the crew tried to ward off the attackers with a butcher knife.

C. VULNERABILITIES OF XML SECURITY

All technologies employed have a measure of vulnerability associated with their implementation. Vulnerabilities are based upon the surface area accessible for attack, the transmission medium, the interaction methods and technology by which messages are passed, etc. Vulnerabilities can be a direct attack against the specification or attacks against the variations in implementation. In the view of the author, there it is a fools mission is to declare that a given technology and its associated implementations are perpetually secure and lack vulnerabilities. This section briefly covers a few of the vulnerabilities associated with the technology. It is not all encompassing . (Hill 2007)

1. Man-in-the-Middle

XKMS is vulnerable to the man-in-the-middle attack during initial key exchange. Party A wants to communicate with part B but uninvited party C wants to listen in. If party A sends the request to communicate to party B, but party C intercepts and masquerades as party A to party B, then party B forwards its credentials to party A via party C. When the handshake is complete, party A believes its talking to party B, but it is in fact talking to party C who is relaying information to party C such that all data transmitted is visible to party C.

2. Improper Implementation of XML Security

Proper implementations of security protocols are an essential factor in applicable security factors. A document that is compressed using EXI compression cannot be encrypted using XML encryption because it is no longer an XML document once compressed. Likewise, the order of operations is of concern when using XML digital signature. The hash of the document is never taken before C14N processing else the digital signature would be invalid.

Within the XML Encryption specification, there exists a set of optional elements that present an opportunity for a key to be sent in the clear. If a key is ever distributed in the clear without any form of encryption applied, then all traffic transmitted using the key must be considered compromised. If the organization policy is to include the key in the clear as part of the transmission, then what is the point of securing the document in relations to confidentiality? It may never be achieved (W3C Encryption Working Group).

3. Frequency Analysis Attack

A major component of any cryptographic algorithm is its degree of entropy in regards to ciphertext. Entropy is the degree of randomness produced by the encryption routine. By studying the patterns of the ciphertext a pattern might be discovered that may reveal clues to the plaintext. Ciphertext is encrypted text wheras plaintext is the original message. Within the English language, there are a plethora of words containing the subset of common combinations of letters such as {“th”, “ing”, “sc”, “ph”, “fr”, “ed” etc.}. A pattern of these common charactersets may emerge in the ciphertext thereby revealing the plaintext. Based upon the cryptographic algorithm selected, XML encryption may be vulnerable to a frequency analysis attack. This is an attack on the algorithm and not XML encryption in general.

4. Element Wrapping Attacks

Based upon the approach used, an XML signed document is prone to an element wrapping attack if only a portion of the document is signed. The remaining portions are left unprotected and vulnerable to modification. Therefore, it is recommended that the full document be signed whenever possible (Hill 2007).

5. Untrusted Keys

Although not an attack on the specification, this is an attack on the application processing the document. Anyone that has access to the appropriate software and hardware can create and sign a key. Therefore, the applications in practice must have a method of resolving the keys via some method of establishing a trust authority. Pretty Good Privacy (PGP) is an option whose trust is established via a ring of faith. For example, if Bob trust Jack and Jack trust Alice then Bob Trusts Alice. Everyone that is contained within the ring of Trust is vetted by another entity that is trusted by someone that they know. Now, if the symmetry of the trust relation is broken such that Bob trusts Jack but does not trust Alice, but Jack trusts Alice, and Jack's content can be viewed by Alice because of the trust relationship, then that means that there is a potential that Bob's information may also be viewed by Alice, if not properly protected. The impact in the use and acceptance of untrusted keys is a weakened or ineffective encyrption key.

6. Attack on the External Elements of an XML Document

An XML document may utilize one or more references that may not be local to the secure enclave to which it is written. This means that an attack on the reference is an indirect attack on the document, which impacts validation. In an attacker can access a URL to a schema or DTD and change it then any files that rely on it for validation would fail thereby creating a denial of service. If an arbitrary schema pertinent to validation for a given site was altered in a malicious fashion then all XML that was validated by that site would no longer validate against the schema or DTD. This would attack the second step in XML digital signature process, XML validation. Therefore, depending upon the implementation, an indirect attack on the implementation of the XML specification would adversely affect the ability of the originator to generate and XML document and the recipient to successfully to receive an XML document (Hill 2007).

D. STILL-NEEDED FUNCTIONALITY

XML digital signature and XML encryption perform much-needed tasks in the advancement of web services, but further integration with XML-based high performance compression methodology is needed. Extensible binary schema-based compression (XSBC) was a good first start. However, being dependent upon a schema is in itself a weakness in that not all XML would be able to benefit from the technology. Efficient XML Interchange (EXI) is a step further in the right direction but once it has been processed under EXI it cannot be encrypted using XML Encryption. Therefore, further integration with the XML specification is required to support the full integration of EXI in XML Encryption technologies.

E. SUMMARY

XML Digital Signature and XML Encryption is useful in coordinating activities between civilian and government agencies. Used in conjunction with XMPP, XML security offers a robust array of features that enables secure realtime chat. However, XML Security is not without vulnerabilities. Several vulnerabilities can be mitigated with appropriate approach selection, implementation techniques and procedures. Indirect attacks are also valid but in-depth discussion is beyond the scope of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The XML digital signature, efficient extensible markup language interchange (EXI), and encryption specification provides a robust framework to provide an international standard for secure information exchange. The use of EXI makes XML technology viable for providing secure communications across multiple nodes within a bandwidth-constricted environment. EXI is the superior to other compression implementations in that with either schema-based or schemaless compression, results indicate that it has massive performance and compression gains over other methods.

The application of XML digital signature provides message and document integrity via the generation of the message digest, authenticity through the combination of the message digest with the private key, and signer authentication via the public private key pair. XML encryption provides message confidentiality.

XML security is a primary contender to become an international standard because it is a license-free, platform-independent and well-supported technology that is modular and designed for structuring data (Boss). It can interface with multiple other formats through the use of XLST, thereby, reducing the requirement for expedited integration of new structures within an economic repressed society. The modularity of XML facilitates full integration with existing command and control suites for national and international messaging. COE CMP can generate XML MTF messages and can also process and support messages generated for NATO operations as well as other coalition operations. Therefore, the application of XML Encryption and Authentication works all variants of XML. XML security provides a lightweight infrastructure that can apply various cryptographic algorithms to satisfy the prevalent security policy while simultaneously providing a framework for global interoperability through a standards-based approach to security.

The application of applying security at the document and message level enhances security of the material being transmitted. Security at the document level increases the cost of infiltration to the would-be attacker and increases. The signatures applied to the document would remain valid with the document until the document has been changed in which case the signature would no longer be valid. However, unaltered digitally signed documents can be used for several legal matters inclusive of non-repudiation.

The drawback of using discretionary access control (DAC) is that once the sender releases the document, he or she no longer has control of the document. Therefore, a trust relationship must exist between the sender and recipients. In particular, the sender must trust that the recipient does not violate standing agreement and use the information for the purpose it was sent. Nonetheless, sometimes these issues are unavoidable i.e., depending upon implementation, if (Alice trusts Bob) and (Bob trusts Alice) and (Alice trusts Charlie) and (Charlie trusts Alice), then it follows that (Bob trusts Charlie by association with Alice). However, if Bob does not trust Charlie, but Alice trusts Charlie, then protocols must be established, such that documents entrusted and accessible by Alice are not accessible to Charlie.

B. RECOMMENDATIONS FOR FUTURE WORK

The following is a list of topics for future research:

- Certification and accreditation of XML Encryption and Authentication for the unclassified architecture. XML is new but not that new therefore, it needs to be properly vetted by an non-partisan official certification and accreditation authority such that the technology can be adopted by sovereign powers as an official alternative for communications.
- Applicability of XML Digital Signature and XML Encryption for real web time services in relation to continued use of Secure Sockets Layer (SSL). This thesis covered embedded security with XML documents. However, the technology can be adopted to compare and contrast Web Services in relation to secure sockets layer in terms of technologicial development, cost, and moving parts. XML in general has far more surface area than

SSL, but it does a great deal more. Web Services encompasses these XML Digital Signatures and XML Encryption and makes this a viable area for continued study.

- Application of XML encryption and authentication with the classified arena. Although a thorough study of the vulnerabilities associated with XML encryption and authentication should be conducted prior to any discussion of applying the technology within either a multilevel security or classified environment, the process at its core does have the same methodology but on different platforms. Each browser and associated XML implementation as well as a thorough analysis of the underlying protocols need to be explored via formal methods. Only a formal method methodology may give entities seeking to preserve data the assurance they require that the techniques employed may not compromise their security.
- A comparative analysis and potential for document centric XML Security in support of CENTRIX and COSMOS. In 2007 JTIC performed an analysis of COSMOS and declared it a promising technology that needed improvement. It was based on routers and VPN technologies. However, changing the technology to embed the security within the XML message itself may affect transmissions and delivery of messages in a more positive manner.
- An in-depth analysis of how message-based and document-centric security using XML authentication and encryption can be integrated with Security Assertion Markup Language (SAML). SAML, provided by Organization for the Advancement of Structured Information Standards (OASIS), is generally known for its single sign-on abilities. However, single sign-on is merely one of the capabilities of SAML. However, if multifactor security is the goal, the application of SAML, with another set of credentials using XML Security, make it more powerful protocol.

- An analysis of XML document-centric security within the Web Services Security infrastructure may provide further insight that decouples security attributes from its respective base platform.

APPENDIX A. EXEMPLAR FILE CONVERSIONS AND MESSAGES

Open source and proprietary tools possess the capability of converting a comma separated value file to a well-formed valid XML file, as described in Chapter IV. The resultant structured data is ready to be used by any application that accepts its format.

A. FULL XML FILE REPRESENTATION OF CSV DATA FILE FROM CHAPTER IV FIGURE 35

```
<?xml version="1.0" encoding="UTF-8"?>
<Import>
    <Row>
        <FirstName>John</FirstName>
        <MiddleInitial>Phineas</MiddleInitial>
        <LastName>Doe</LastName>
        <Rank>CAPT</Rank>
        <Service>USN</Service>
        <Location>USS Bainbridge</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Peter</FirstName>
        <MiddleInitial>Demetrius</MiddleInitial>
        <LastName>Jones</LastName>
        <Rank>LCDR</Rank>
        <Service>USCG</Service>
        <Location>USS Comanche</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Mathais</FirstName>
        <MiddleInitial>Plasidius </MiddleInitial>
        <LastName>Montique</LastName>
        <Rank>GS-15</Rank>
        <Service>DOD</Service>
        <Location>Mombassa, Kenya</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Ameila</FirstName>
        <MiddleInitial>NMN</MiddleInitial>
        <LastName>Starr</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>Fulton Co., GA</Location>
        <Status>Deceased 99</Status>
    </Row>
    <Row>
```

```
        <FirstName>Floyd</FirstName>
        <MiddleInitial>Morgan</MiddleInitial>
        <LastName>Williams </LastName>
        <Rank>CIV</Rank>
        <Service>Clergy</Service>
        <Location>Boston, MA</Location>
        <Status>Deceased 06</Status>
</Row>
<Row>
        <FirstName>Tang</FirstName>
        <MiddleInitial>Vu</MiddleInitial>
        <LastName>Chiang</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>Siagon, Vietnam</Location>
        <Status>Up</Status>
</Row>
<Row>
        <FirstName>Awanstar</FirstName>
        <MiddleInitial>Schaeffer</MiddleInitial>
        <LastName>Lines</LastName>
        <Rank>CIV</Rank>
        <Service>Contractor</Service>
        <Location>Detroit, MI</Location>
        <Status>Up</Status>
</Row>
<Row>
        <FirstName>Eunice</FirstName>
        <MiddleInitial>Kennedy</MiddleInitial>
        <LastName>Schriver</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>Monterey, CA</Location>
        <Status>Deceased 09</Status>
</Row>
<Row>
        <FirstName>Rovert</FirstName>
        <MiddleInitial>F</MiddleInitial>
        <LastName>Kennedy</LastName>
        <Rank>Commander-in-Chief</Rank>
        <Service>US</Service>
        <Location>Washington, DC</Location>
        <Status>Deceased 72</Status>
</Row>
<Row>
        <FirstName>Ferdinand</FirstName>
        <MiddleInitial>Dubia</MiddleInitial>
        <LastName>Cascinco</LastName>
        <Rank>1st LT</Rank>
        <Service>USA</Service>
        <Location>Ciaro, Egypt</Location>
        <Status>Up</Status>
</Row>
<Row>
        <FirstName>Geoffrey</FirstName>
        <MiddleInitial>Xavier</MiddleInitial>
        <LastName>Parsons</LastName>
        <Rank>SGT</Rank>
        <Service>LAPD</Service>
        <Location>Los Angelos, CA</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Felipa</FirstName>
        <MiddleInitial>Cordoves</MiddleInitial>
        <LastName>Kerr</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>San Diego, CA</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Christina</FirstName>
        <MiddleInitial>Sunshine</MiddleInitial>
        <LastName>Johnson</LastName>
        <Rank>CIV</Rank>
        <Service>USN Dependent</Service>
        <Location>San Diego, CA</Location>
        <Status>Deceased 90</Status>
    </Row>
    <Row>
        <FirstName>Timothy</FirstName>
        <MiddleInitial>Antwoine</MiddleInitial>
        <LastName>Cooper</LastName>
        <Rank>GYST</Rank>
        <Service>USMC</Service>
        <Location>Newport, RI</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Antonio</FirstName>
        <MiddleInitial>Steamer</MiddleInitial>
        <LastName>Anderson</LastName>
        <Rank>LCDR</Rank>
        <Service>USN</Service>
        <Location>Baltimore, MD</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Vitterio</FirstName>
        <MiddleInitial>Julius</MiddleInitial>
        <LastName>Crisp</LastName>
        <Rank>CDR</Rank>
        <Service>USN</Service>
        <Location>Sigonella, Sicily</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Julius</FirstName>
        <MiddleInitial>Von</MiddleInitial>
        <LastName>Ceasar</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>Naples, Italy</Location>
        <Status>Deceased 88</Status>
    </Row>
    <Row>
        <FirstName>Loren</FirstName>
        <MiddleInitial>Jascupisco</MiddleInitial>
        <LastName>Peterson</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>Beaumont, TX</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Eula</FirstName>
        <MiddleInitial>Janet</MiddleInitial>
        <LastName>Praylor</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>Guam</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Adorn</FirstName>
        <MiddleInitial>Vanessa</MiddleInitial>
        <LastName>Johnson</LastName>
        <Rank>CIV</Rank>
        <Service>N/A</Service>
        <Location>Manilla, Philipines</Location>
        <Status>Up</Status>
    </Row>
    <Row>
        <FirstName>Breanna</FirstName>
        <MiddleInitial>Naiomi </MiddleInitial>
        <LastName>Santos</LastName>
        <Rank>MAJ</Rank>
        <Service>USA</Service>
        <Location>Muscat, Oman</Location>
        <Status>Up</Status>
    </Row>
</Import>
```

XML is a structured modular language that facilitates data extraction and customization. By extracting only the portion that is required, data customization is achieved. It is performed natively via an XSLT or with some other open source or proprietary customizable tool.

B. XML OUTPUT OF FILE GENERATED BY XSLT FILE FROM CHAPTER IV FIGURE 36

```
<?xml version="1.0" encoding="UTF-8"?>
<Import>
        <Officer>
                <Rank>CAPT</Rank>
                <LastName>Doe</LastName>
        </Officer>
        <Officer>
                <Rank>LCDR</Rank>
                <LastName>Jones</LastName>
        </Officer>
        <Officer>
                <Rank>GS-15</Rank>
                <LastName>Montique</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Starr</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Williams </LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Chiang</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Lines</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Schriver</LastName>
        </Officer>
        <Officer>
                <Rank>Commander-in-Chief</Rank>
                <LastName>Kennedy</LastName>
        </Officer>
        <Officer>
                <Rank>1st LT</Rank>
                <LastName>Cascinco</LastName>
        </Officer>
        <Officer>
                <Rank>SGT</Rank>
                <LastName>Parsons</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Kerr</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Johnson</LastName>
        </Officer>
        <Officer>
                <Rank>GYST</Rank>
                <LastName>Cooper</LastName>
        </Officer>
        <Officer>
                <Rank>LCDR</Rank>
                <LastName>Anderson</LastName>
        </Officer>
        <Officer>
                <Rank>CDR</Rank>
                <LastName>Crisp</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Ceasar</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Peterson</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Praylor</LastName>
        </Officer>
        <Officer>
                <Rank>CIV</Rank>
                <LastName>Johnson</LastName>
        </Officer>
        <Officer>
                <Rank>MAJ</Rank>
                <LastName>Santos</LastName>
        </Officer>
</Import>
```

Organizations require coordination between participating entities to ensure that each participant is clear on their role and responsibilities for specific events. This also serves as the venue for participating entities to discuss items of concerns to include capabilities, limitations, policy differences, etc. Such meetings assist the principle organization in creating the ideal structure. Visit request are critical to assure that all participants can communicate at the requisite security level to engage other members attending in additional to being able to attend all briefings. The following message is an example of a notional visit request that would be sent from one organization to another.

C. ACP-126 USMTF VISIT REQUEST

```
UNCLASSIFIED
MSGID/VISITREQ/NATO BRUSSELS/-/MAR//
REF/A/MSGID:GENADMIN/NAVPGSCOL MONTEREY CA/YMD:20040319//
AMPN/REF MUILTINATIONAL ANTIPIRACY COORDINATION CONFERENCE//
VISITREQ/CONTACT:MS. BOYD/PRIPHN:DSN 773-
7583/BEGDAY:19JAN2005
/ENDDAY:25JAN2005/-/-/CLAS:CONFIDENTIAL//
GENTEXT/VISIT PURPOSE/ANTIPIRACY CONF//
LOCSITE/UNIT:CCSG12/PHUKET THIALAND//
PERSDAT/HARD U.P./LCDR/SSAN:012345678/S/SAN DIEGO,
CA/23MAY1975/US//
GRANTOR/DONCAF/29AUG2002//
PERSDAT/-BYTE M.E./CIV/SSAN:754627532/TS/DES MOINES,
IA/22JAN1962/US
//
GRANTOR/CCF/05FEB2004//
POC/CEASAR, J/CDR/NATO SHAPE MIL CMTE/LOC:SHERATON, PHUKET
/TEL:DSN 563-
6426/EMAIL:CEASARJ(AT)USDELAGTIONAUTHTHIA.US.GOV//
```

XML is a verbose structured language and therefore has more levels of granularity than data contained in other formats. Due to this nature, XML data can easily be parsed and customizable subsets of data can be pulled from their overall file with little effort.

D. COMMON OPERATING ENVIRONMENT COMMON MESSAGE PROCESSOR (COE CMP) GENERATED XML REPRESENTATION OF VISIT REQUEST

```
<?xml version="1.0"?>
<mtf:visit_request
   xmlns:mtf="urn:mtf:mil:usmtf:2004"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <message_identification>
      <message_text_format_identifier>VISITREQ</message_text_format_identifier>
      <originator>NATO BRUSSELS</originator>
      <month_name>MAR</month_name>
   </message_identification>
   <reference>
      <amplification>
         <free_text xml:space = 'preserve'>REF MUILTI NATIONAL ANTIPIRACY COORDINATION
CONFERENCE</free_text>
      </amplification>
      <serial_identifier>A</serial_identifier>
      <type_of_reference>
         <message_text_format_identifier>GENADMIN</message_text_format_identifier>
      </type_of_reference>
      <originator>NAVPGSCOL MONTEREY CA</originator>
      <date_and_or_time_of_reference>
         <date_of_reference_year_month_day>
            <year>2004</year>
            <month_numeric>03</month_numeric>
            <day>19</day>
         </date_of_reference_year_month_day>
      </date_and_or_time_of_reference>
   </reference>
   <visit_request>
      <point_of_contact_name>MS. BOYD</point_of_contact_name>
      <primary_telephone_number>DSN 773-7583</primary_telephone_number>
      <visit_begin_date_day_alphamonth_year>
         <day>19</day>
         <month_name>JAN</month_name>
         <year>2005</year>
      </visit_begin_date_day_alphamonth_year>
      <visit_end_date_day_alphamonth_year>
         <day>25</day>
         <month_name>JAN</month_name>
         <year>2005</year>
      </visit_end_date_day_alphamonth_year>
      <discussion_information_classification>CONFIDENTIAL</discussion_information_classification>
   </visit_request>
   <general_text_information_1>
      <gentext_text_indicator>VISIT PURPOSE</gentext_text_indicator>
   <free_text xml:space ='preserve'>ANTIPIRACY CONF</free_text>
</general_text_information_1>
<visit_site_location_data>
   <facility_location_unit_name>
      <unit_name>CCSG12</unit_name>
   </facility_location_unit_name>
   <sub_organization_identifier>PHUKET THIALAND</sub_organization_identifier>
</visit_site_location_data>
<personnel_data_and_clearance_segment>
   <personnel_data_and_clearance>
      <name_of_individual>HARD U.P.</name_of_individual>
      <military_rank_rating_or_grade>LCDR</military_rank_rating_or_grade>
      <social_security_number_or_service_number>
         <social_security_number>012345678</social_security_number>
      </social_security_number_or_service_number>
      <security_clearance>S</security_clearance>
      <birthplace>SAN DIEGO, CA</birthplace>
      <birthdate_day_alphamonth_year>
         <day>23</day>
         <month_name>MAY</month_name>
         <year>1975</year>
      </birthdate_day_alphamonth_year>
      <nationality>US</nationality>
   </personnel_data_and_clearance>
   <security_clearance_grantor_data>
      <security_clearance_granting_agency>DONCAF</security_clearance_granting_agency>
      <date_clearance_granted_day_alphamonth_year>
         <day>29</day>
         <month_name>AUG</month_name>
         <year>2002</year>
      </date_clearance_granted_day_alphamonth_year>
   </security_clearance_grantor_data>
</personnel_data_and_clearance_segment>
<personnel_data_and_clearance_segment>
   <personnel_data_and_clearance>
      <name_of_individual>-BYTE M.E.</name_of_individual>
      <military_rank_rating_or_grade>CIV</military_rank_rating_or_grade>
      <social_security_number_or_service_number>
         <social_security_number>754627532</social_security_number>
      </social_security_number_or_service_number>
      <security_clearance>TS</security_clearance>
      <birthplace>DES MOINES, IA</birthplace>
      <birthdate_day_alphamonth_year>
         <day>22</day>
         <month_name>JAN</month_name>
         <year>1962</year>
      </birthdate_day_alphamonth_year>
      <nationality>US</nationality>
   </personnel_data_and_clearance>
   <security_clearance_grantor_data>
      <security_clearance_granting_agency>CCF</security_clearance_granting_agency>
      <date_clearance_granted_day_alphamonth_year>
         <day>05</day>
         <month_name>FEB</month_name>
         <year>2004</year>
      </date_clearance_granted_day_alphamonth_year>
    </security_clearance_grantor_data>
  </personnel_data_and_clearance_segment>
  <point_of_contact_information>
    <contact_name>CEASAR, J</contact_name>
    <rank_or_position>CDR</rank_or_position>
    <unit_identifier_or_call_sign>
      <unit_identifier>NATO SHAPE MIL CMTE</unit_identifier>
    </unit_identifier_or_call_sign>
    <poc_location>
      <location_name>SHERATON, PHUKET</location_name>
    </poc_location>
    <group_of_fields>
      <telephone_number_or_frequency>
        <nonsecure_telephone_number>DSN 563-6426</nonsecure_telephone_number>
      </telephone_number_or_frequency>
    </group_of_fields>
    <group_of_fields>
      <telephone_number_or_frequency>

<electronic_mail_address>CEASARJ(AT)USDELAGTIONAUTHTHIA.US.GOV</electronic_mail_addre
ss>
      </telephone_number_or_frequency>
    </group_of_fields>
  </point_of_contact_information>
</mtf:visit_request>
```

E. ACP-126 USMTF INITIAL PLANNING CONFERENCE (IPC)

Most events requires a planning conference to investigate the best course of action, areas of responsibility and available assets. In conducting such conference, the task force commander is endowed with sufficient information to draft coordinate the projection of proper assets within the appropriate locations within the battlespace. For example, if an attack is in progress and is in excess of 50 miles away, either a fixed wing or helicopter may be tools of choice. The object is to reduce the response time of an attack within the area of interest to a few minutes thereby making it extremely expensive to the adversary to conduct operations within the vicinity of the Horn of Africa.

```
UNCLASSIFIED
MSGID/GENADMIN/ESG2/-/JUN//
SUBJ/NOTIFICATION OF ANTIPIRACY SOUTHERN WATCH INITIAL PLANNING
/CONFERENCE//
POC/CDR OMAR DENZEL/FPO/ESG2/-/TEL:001-757-445-9595/TEL:312-565-8750
/TEL:001-757-621-6352/EMAIL:OMAR.DENZEL@NAVY.MIL//
GENTEXT/REMARKS/1. AUTHORIZATION GRANTED BY NAVEUR AND SIXTH FLEET
FOR CTF151 TO SEND SUBJ MSG TO USDAOS. REQUEST USDAOS DISSEMINATE
THIS MESSAGE TO APPROPRIATE HOST NATION COMMANDS AND STAFFS.
2.COMMANDER, AMPHIBIOUS STRIKE GROUP TWO WILL HOST THE INITIAL
PLANNING CONFERENCE (IPC) AT THE SHERATON WATERSIDE HOTEL
3. MISSION OVERVIEW:   THE INTERNATIONAL COMMUNITY IS CURRENTLY
UNDER ATTACK BY A NON-TRADITIONAL ADVERSARY.  THE ADVERSARY IS NOT A
SOVERIEGN ENTITY BUT THIEVES AND MURDERERS THEY PREY ON DEFENSELESS
MERCHANT AND PRIVATELY OWNED VESSELS.  THE ADVERSARY RESPECTS NO
AUTHORITY. IT'S MOTIVATION IS NEITHER POLITICAL NOR TERROR BUT IT IS
GREED.  THE ADVERSARY IS EVERY NATION'S ARCH ENEMY FROM TI’MES
ANCIENT TIMES.  IT IS THE MODERN DAY PIRATE.
THE ASSEMBLED MULTINATIONAL TASK FORCE IS A HQ USEUCOM DIRECTED,
COMUSNAVEUR
MARITIME AND LAND OPERATIONS WILL BE HELD IN THE HORN OF AFRICA AREA
CONTINUOUSLY TILL THE THREAT IS ELIMINATED.  MAKE NO MISTAKE ABOUT
IT WE ARE IN FOR THE LONG HALL.  COMMAND WILL ROTATE BETWEEN MEMBER
NATIONS.  THE PRIMARY PLANNING, COORDINATION AND EXECUTION
COMMAND IS COMMANDER, AMPHIBIOUS STRIKE GROUP TWO.
4. THE FOLLOWING NATIONS ARE INVITED TO SEND NAVY AND MARINE
REPRESENTATIVES TO THE IPC: DENMARK, ESTONIA, FINLAND, FRANCE,
GERMANY, LATVIA, LITHUANIA, NORWAY, POLAND, RUSSIA, SWEDEN, UNITED
KINGDOM, CHINA, ISREAL, BAHRAIN, UAE, PAKISTAN, IRAN, SOMOLIA,
SPAIN, SOUTH AFRICA, JAPAN, ITALY, UNITED STATES.
   A. FURTHER, NATIONS ARE INVITED TO PROVIDE REPRESENTATIVES TO
DISCUSS SPECIFIC ISSUES AT WORKING GROUPS AS FOLLOWS:
     EXERCISE CONTROL GROUP/ROE: ALL
     COMMUNICATIONS: ALL
     SURFACE: NATIONS OFFERING SURFACE FORCES
     AIR: CAOC-1 AND NATIONS OFFERING AIR FORCES
     SUBSURFACE: CINCGERFLEET AND NATIONS OFFERING SUBMARINE
        ASSETS OR VARIABLE DEPTH SONAR SHIPS
     LAND: USMC 2-23, MARFOREUR AND NATIONS OFFERING LAND FORCES
     AMPHIB: USMC 2-23, MARFOREUR AND NATIONS OFFERING AMPHIBIOUS
        SHIPPING
     OPFOR: UK (HMS SUTHERLAND)
```

LOGISTICS: ALL
MCM: UK (MCM HQ) AND NATION OFFERING MCM FORCES

ESG-2 RECOGNIZES THAT IT MAY NOT BE PRACTICAL FOR ALL NATIONS TO SEND REPRESENTATIVES TO ALL WORKING GROUPS LISTED ABOVE. HOWEVER, IT IS REQUESTED THAT THE DESIGNATED IPC REPRESENTATIVES BE SUFFICIENTLY KNOWLEDGEABLE TO PROVIDE INPUT TO THE ABOVE WORKING GROUPS.

B. ACTION OFFICER PARTICIPATION/KEY PLANNING DATES ARE 7-9 DEC.

C. ACTION OFFICERS MUST BE PREPARED AND AUTHORIZED TO MAKE DECISIONS REGARDING COMMAND AND CONTROL ARRANGEMENTS AND OTHER ISSUES LISTED AS IPC OBJECTIVES.

5. ADDRESSEES ARE REQUESTED TO FORWARD A LIST OF PARTICIPANTS TO ESG-2 POC (PARA 10.H.) BY 20 NOVEMBER, 2004 IN THE FOLLOWING FORMAT:

(1) NAME/RANK/SERVICE
(2) NATION/COMMAND REPRESENTED
(3) CONTACT PHONE NUMBER/EMAIL ADDRESS
(4) WORKING GROUP(S) TO ATTEND
(5) SPECIFIC TACTICAL OBJECTIVES

REQUEST USDAO ADDRESSEES PROVIDE POC FOR BALTOPS ISSUES TO ESG-2 POC TO FACILITATE FOLLOW ON COMMUNICATIONS.

6. OBJECTIVES OF THE IPC ARE:

A. FINALIZE COMMAND AND CONTROL, WORKING GROUP ASSIGNMENTS AND TASK ORGANIZATION
B. PROPOSE AND APPROVE DRAFT INITIAL TASKING ORDERS
C. COMMENCE PLANNING AND FUNCTIONAL COMMANDER
D. BEGIN DEVELOPMENT OF C4I STRUCTURE TO SUPPORT C2 ORGANIZATION
E. ASSIGN OPORDER DEVELOPMENT RESPONSIBILITIES
F. COORDINATE HELO INTEROPERABILITY. ALL PARTICIPANTS OFFERING HELO CAPABLE SURFACE PLATFORMS SHOULD BRING APPROPRIATE TECHNICAL DATA FOR HELO FLIGHT DECK CAPABILITY AND VERIFY NATO HOSTAC COMPATIBILITY (IF APPLICABLE).

7. IN PREPARATION FOR THE IPC REQUEST THAT EACH PARTICIPATING NATION PROVIDE THE FOLLOWING NLT 20 NOV:

A. AVAILABLE LAND RANGES TO CNE/C6F POC (PARA 10.H.).

B. INPUTS ON POSSIBLE PORTS AVAILABLE TO ACCOMMODATE THE PRE-SAIL AND POST SAIL EXERCISES TO CNE/C6F POC.

C. PARTICIPANTS TO HOST THE MPC CONTACT CNE/C6F POC.

D. PARTICIPANTS CONFIRM AVAILABILITY FOR LISTED WORKING GROUP AND COMMAND AND CONTROL ASSIGNMENT TO ESG-2 POC.

E. SPECIAL EVENTS. AGREEMENT ON STRUCTURE OF THE SERIAL PHASE WILL BE ACHIEVED AT THE IPC. SPECIFIC TACTICAL OBJECTIVES, TACTICS VALIDATION OR SERIALS TO BE INCLUDED IN THE SERIAL PHASE ARE TO BE PROVIDED AT THE IPC.

F. UPDATED FORCE PARTICIPATION. REQUEST EACH NATION PROVIDE ANY CHANGES TO FORCE OFFERINGS DISCUSSED AT CDC TO ESG-12 POC BY 20 NOV 2004.

8. WORKING GROUP LEADS. TENTATIVE WORKING GROUP LEAD ASSIGNMENTS:

A. EXERCISE CONTROL GROUP/ROE: US - ESG-12
B. AIR: US, FRANCE AND GERMANY - CAOC-1
C. SURFACE: US - ESG-12
D. SUBSURFACE: GE - CINCGERFLEET
E.–LAND: US - USMC 2-23
F. OPFOR: UK - HMS SUTHERLAND
G. LOGISTICS: US - ESG-2
H. COMMUNIICATIONS/OPSEC: US AND GERMANY - ESG-2 AND CINCGERFLEET
I. MCM: UK - MCM HQ
J.AMPHIB:– US - LSD/LPD (TBD)

WORKING GROUP LEAD WILL PROVIDE DIRECTION AND OVERSIGHT.

9. SCHEDULE OF EVENTS FOR BALTOPS 2005 IPC FOLLOWS:

6 DECEMBER (MONDAY)

TRAVEL DAY FOR ALL PARTICIPANTS

----

7 DECEMBER (TUESDAY)

0730-0815 CHECK-IN SHERATON CONFERENCE ROOM

0815 OPENING REMARKS BY ESG-12 AND INTRODUCTION

0830 CONFERENCE ADMIN/OVERVIEW

0840 COUNTRY/FORCE REPRESENTATIVE INTRODUCTIONS

0920 REVIEW CDC NOTES (C6F)/REVIEW IPC OBJECTIVES AND REQUIREMENTS

1000 PRESENTATION OF COMMAND AND CONTROL, WORKING GROUP ASSIGNMENTS AND OPORDER RESPONSIBILITIES

1030 TACTICAL PLANNING BRIEF

1230 DRAFT INITIAL PLANNING ORDERS

1300 SERIAL BRIEF

1330 WORKING GROUP OBJECTIVES

1345-1500 WORKING GROUP MEETINGS

1500-1600 WORKING GROUP PROGRESS REPORTS

1800-2000 RECEPTION HOSTED BY ESG-12 (SHERATON) (DRESS: CASUAL)

----

8 DECEMBER (WEDNESDAY)

0800 DAY ONE REVIEW AND DAY TWO OBJECTIVES

0830 ROE OVERVIEW

0900 PROPOSED TASK FORCE ORGANIZATION

0930 WORKING GROUP MEETINGS

1500-1530 WORKING GROUP PROGRESS REPORTS

----

9 DECEMBER (THURSDAY)

0800 DAY TWO REVIEW AND DAY THREE OBJECTIVES

0815 WORKING GROUP MEETINGS

1000 WORKING GROUP OUTBRIEFS

1400 IPC OBJECTIVES STATUS REVIEW

1430 ROADMAP, MPC AGENDA/LOGISTICS

1500 IPC WRAP-UP

----

10 DECEMBER (FRIDAY)

TRAVEL DAY FOR ALL PARTICIPANTS

10. ADMINISTRATION.

A. WEBSITE ACCESS: COMMANDS DESIGNATE 2-3 PERSONNEL TO OBTAIN ACCESS TO THE HOA IN THE PARTNERS FOR PEACE INFORMATION MANAGEMENT SYSTEM (PIMS) WEBSITE. THE FIRST STEP IS TO REGISTER AND OBTAIN AN ACCOUNT AND PASSWORD. TO REGISTER GO TO THE FOLLOWING SITE: HTTP: (DOUBLE
IN THE REMARKS SECTION. ONCE YOU HAVE OBTAINED AN ACCOUNT GO TO THE PIMS HOME PAGE AND SELECT BALTOPS UNDER THE ANNOUNCEMENT BANNER (PASSWORD PROTECTED). THIS IS WHERE ALL PERTINENT DOCUMENTS RELATING TO HOA SOTHERN WATCH WILL BE POSTED.

B. CONFERENCE. ROOM WILL BE EQUIPPED TO SUPPORT MICROSOFT POWERPOINT BRIEFS WITH A PROJECTOR. ESG-2 OPERATES POWERPOINT 2003. COMMANDS PROVIDING POWERPOINT BRIEFS, EMAIL BRIEFS TO ESG-2 POC NLT 20 NOV. MAX FILE ATTACHMENT SIZE IS 5MB. FILE MAY BE MAILED TO POC AT:

CDR OMAR DENZEL
COMMANDER EXPEDITIONARY STRIKE GROUP TWO
UNIT 123456
FPO AE 09506-4704

C. SHERATON WATERSIDE HOTEL

(1) SHERATON PHUKETPHUKET, THAILAND. RESERVATIONS CAN BE MADE DIRECT TO THE HOTEL AT 011-757-622-6664. FAX NUMBER IS 011-757-635-8271. WEBSITE IS HTTP (SLASH SLASH)WWW.PHUKET.COM/SHERATON/. FORTY (40) ROOMS ARE SET ASIDE FOR THE CONFERENCE. ROOM CHARGE IS ONE HUNDRED AND TEN (110) US PER NIGHT PLUS APPLICABLE TAXES AND FEES.

(2) REQUEST THAT “SOUTHERN WATCH” IS REFERENCED WHEN BOOKING RESERVATIONS. TO ENSURE ADEQUATE AVAILABILITY, ATTENDEES ARE ENCOURAGED TO MAKE RESERVATIONS NO LATER THAN 12 NOV 2004.

(3) A CONFERENCE FEE OF TEN (10) US DOLLARS WILL BE COLLECTED DURING CHECK-IN TUESDAY MORNING 7 DEC TO COVER ADMINISTRATIVE COSTS.

D. FOR TRANSPORTATION ISSUES PLEASE CONTACT THE ESG-2 STAFF DUTY OFFICER AT 757-642-6970. ADDITIONALLY, IF ANY ISSUES ARE ENCOUNTERED WITH THE HOTEL, PLEASE CONTACT THE ESG-2 LOGISTICS OFFICER AT 757-946-1234.

F. INFORMATION ON THE PHUKET, THAILAND AREA MAY BE FOUND ON THE WEB AT WWW.PHUKET.COM.

G. ATTIRE. THE CONFERENCE WILL BE CONDUCTED IN WORKING UNIFORM.

H. POINTS OF CONTACT:

C6F-CNE: LT JOSE DELGADOE -N37, DSN: 314-235-4–22, COMM: 0044-207-514-4022, CELL: 0044-773-986-2216, FAX: 0044-207-514-4637, EMAIL: JOSE.DELGADOE@NAVEUR.NAVY.MIL

ESG-2: CDR OMAR DENZEL - N34, DSN 312-445-9–95. COMM: 001-757-445-9595, CELL: 001-757-621-6352, FAX: 001-757-445-8703, EMAIL:OMAR.DENZEL@NAVY.MIL//

F. COE CMP GENERATED XML REPRESENTATION OF IPC

```
<?xml version=”1.0”?>
<mtf:general_administration_message
xmlns:mtf=”urn:mtf:mil:usmtf:2”04”
xmlns:xsi=”http://www.w3.org/20”01/XMLSchema-instance”>
<message_identification>

<message_text_format_identifier>GENADMIN</message_text_format_identifier
>
    <originator>ESG2</originator>
    <month_name>JUN</month_name>
  </message_identification>
  <subject>
    <message_subject>NOTIFICATION OF ANTIPIRACY SOUTHERN WATCH INITIAL
PLANNING</message_subject>
    <group_of_fields>
      <message_subject_continued>CONFERENCE</message_subject_continued>
    </group_of_fields>
  </subject>
  <point_of_contact_information>
    <contact_name>CDR OMAR DENZEL</contact_name>
    <rank_or_position>FPO</rank_or_position>
    <unit_identifier_or_call_sign>
      <unit_identifier>ESG2</unit_identifier>
    </unit_identifier_or_call_sign>
        <poc_location   xsi:nil=”true”/>

    <group_of_fields>
      <telephone_number_or_frequency>
        <nonsecure_telephone_number>001-757-445-
9595</nonsecure_telephone_number>
      </telephone_number_or_frequency>
    </group_of_fields>
    <group_of_fields>
      <telephone_number_or_frequency>
        <nonsecure_telephone_number>312-565-
8750</nonsecure_telephone_number>
      </telephone_number_or_frequency>
    </group_of_fields>
    <group_of_fields>
      <telephone_number_or_frequency>
        <nonsecure_telephone_number>001-757-621-
6352</nonsecure_telephone_number>
      </telephone_number_or_frequency>
    </group_of_fields>
    <group_of_fields>
      <telephone_number_or_frequency>

<electronic_mail_address>OMAR.DENZEL@NAVY.MIL</electronic_mail_address>
      </telephone_number_or_frequency>
    </group_of_fields>
  </point_of_contact_information>
  <general_text_information>
    <gentext_text_indicator>REMARKS</gentext_text_indicator>
    <free_text xml:space =’preserve’>1. AUTHORIZATION GRANTED BY NAVEUR
AND SIXTH FLEET FOR CTF151 TO SEND SUBJ MSG TO USDAOS. REQUEST USDAOS
DISSEMINATE THIS MESSAGE TO APPROPRIATE HOST NATION COMMANDS AND STAFFS.
2.COMMANDER, AMPHIBIOUS STRIKE GROUP TWO WILL HOST THE INITIAL
PLANNING CONFERENCE (IPC) AT THE SHERATON WATERSIDE HOTEL
3. MISSION OVERVIEW:   THE INTERNATIONAL COMMUNITY IS CURRENTLY
```

UNDER ATTACK BY A NON-TRADITIONAL ADVERSARY. THE ADVERSARY IS NOT A SOVERIEGN ENTITY BUT THIEVES AND MURDERERS THEY PREY ON DEFENSELESS MERCHANT AND PRIVATELY OWNED VESSELS. THE ADVERSARY RESPECTS NO AUTHORITY. IT&apos;S MOTIVATION IS NEITHER POLITICAL NOR TERROR BUT IT IS
GREED. THE ADVERSARY IS EVERY NATION&apos;S ARCH ENEMY FROM TIMES ANCIENT TIMES. IT IS THE MODERN DAY PIRATE.
THE ASSEMBLED MULTINATIONAL TASK FORCE IS A HQ USEUCOM DIRECTED, COMUSNAVEUR
MARITIME AND LAND OPERATIONS WILL BE HELD IN THE HORN OF AFRICA AREA CONTINUOUSLY TILL THE THREAT IS ELIMINATED. MAKE NO MISTAKE ABOUT IT WE ARE IN FOR THE LONG HALL. COMMAND WILL ROTATE BETWEEN MEMBER NATIONS. THE PRIMARY PLANNING, COORDINATION AND EXECUTION COMMAND IS COMMANDER, AMPHIBIOUS STRIKE GROUP TWO.
4. THE FOLLOWING NATIONS ARE INVITED TO SEND NAVY AND MARINE REPRESENTATIVES TO THE IPC: DENMARK, ESTONIA, FINLAND, FRANCE, GERMANY, LATVIA, LITHUANIA, NORWAY, POLAND, RUSSIA, SWEDEN, UNITED KINGDOM, CHINA, ISREAL, BAHRAIN, UAE, PAKISTAN, IRAN, SOMOLIA, SPAIN, SOUTH AFRICA, JAPAN, ITALY, UNITED STATES.
A. FURTHER, NATIONS ARE INVITED TO PROVIDE REPRESENTATIVES TO DISCUSS SPECIFIC ISSUES AT WORKING GROUPS AS FOLLOWS:
EXERCISE CONTROL GROUP/ROE: ALL
COMMUNICATIONS: ALL
SURFACE: NATIONS OFFERING SURFACE FORCES
AIR: CAOC-1 AND NATIONS OFFERING AIR FORCES
SUBSURFACE: CINCGERFLEET AND NATIONS OFFERING SUBMARINE ASSETS OR VARIABLE DEPTH SONAR SHIPS
LAND: USMC 2-23, MARFOREUR AND NATIONS OFFERING LAND FORCES
AMPHIB: USMC 2-23, MARFOREUR AND NATIONS OFFERING AMPHIBIOUS SHIPPING
OPFOR: UK (HMS SUTHERLAND)
LOGISTICS: ALL
MCM: UK (MCM HQ) AND NATION OFFERING MCM FORCES
ESG-2 RECOGNIZES THAT IT MAY NOT BE PRACTICAL FOR ALL NATIONS TO SEND REPRESENTATIVES TO ALL WORKING GROUPS LISTED ABOVE. HOWEVER, IT IS REQUESTED THAT THE DESIGNATED IPC REPRESENTATIVES BE SUFFICIENTLY KNOWLEDGEABLE TO PROVIDE INPUT TO THE ABOVE WORKING GROUPS.
B. ACTION OFFICER PARTICIPATION/KEY PLANNING DATES ARE 7-9 DEC.
C. ACTION OFFICERS MUST BE PREPARED AND AUTHORIZED TO MAKE DECISIONS REGARDING COMMAND AND CONTROL ARRANGEMENTS AND OTHER ISSUES LISTED AS IPC OBJECTIVES.
5. ADDRESSEES ARE REQUESTED TO FORWARD A LIST OF PARTICIPANTS TO ESG-2 POC (PARA 10.H.) BY 20 NOVEMBER, 2004 IN THE FOLLOWING FORMAT:
(1) NAME/RANK/SERVICE
(2) NATION/COMMAND REPRESENTED
(3) CONTACT PHONE NUMBER/EMAIL ADDRESS
(4) WORKING GROUP(S) TO ATTEND
(5) SPECIFIC TACTICAL OBJECTIVES
REQUEST USDAO ADDRESSEES PROVIDE POC FOR BALTOPS ISSUES TO ESG-2 POC TO FACILITATE FOLLOW ON COMMUNICATIONS.
6. OBJECTIVES OF THE IPC ARE:
A. FINALIZE COMMAND AND CONTROL, WORKING GROUP ASSIGNMENTS AND TASK ORGANIZATION
B. PROPOSE AND APPROVE DRAFT INITIAL TASKING ORDERS
C. COMMENCE PLANNING AND FUNCTIONAL COMMANDER
D. BEGIN DEVELOPMENT OF C4I STRUCTURE TO SUPPORT C2 ORGANIZATION
E. ASSIGN OPORDER DEVELOPMENT RESPONSIBILITIES
F. COORDINATE HELO INTEROPERABILITY. ALL PARTICIPANTS OFFERING HELO CAPABLE SURFACE PLATFORMS SHOULD BRING APPROPRIATE TECHNICAL DATA FOR HELO FLIGHT DECK CAPABILITY AND VERIFY NATO HOSTAC COMPATIBILITY (IF APPLICABLE).

7. IN PREPARATION FOR THE IPC REQUEST THAT EACH PARTICIPATING NATION PROVIDE THE FOLLOWING NLT 20 NOV:

A. AVAILABLE LAND RANGES TO CNE/C6F POC (PARA 10.H.).

B. INPUTS ON POSSIBLE PORTS AVAILABLE TO ACCOMMODATE THE PRE-SAIL AND POST SAIL EXERCISES TO CNE/C6F POC.

C. PARTICIPANTS TO HOST THE MPC CONTACT CNE/C6F POC.

D. PARTICIPANTS CONFIRM AVAILABILITY FOR LISTED WORKING GROUP AND COMMAND AND CONTROL ASSIGNMENT TO ESG-2 POC.

E. SPECIAL EVENTS. AGREEMENT ON STRUCTURE OF THE SERIAL PHASE WILL BE ACHIEVED AT THE IPC. SPECIFIC TACTICAL OBJECTIVES, TACTICS VALIDATION OR SERIALS TO BE INCLUDED IN THE SERIAL PHASE ARE TO BE PROVIDED AT THE IPC.

F. UPDATED FORCE PARTICIPATION. REQUEST EACH NATION PROVIDE ANY CHANGES TO FORCE OFFERINGS DISCUSSED AT CDC TO ESG-12 POC BY 20 NOV 2004.

8. WORKING GROUP LEADS. TENTATIVE WORKING GROUP LEAD ASSIGNMENTS:

A. EXERCISE CONTROL GROUP/ROE: US – ESG-12

B. AIR: US, FRANCE AND GERMANY – CAOC-1

C. SURFACE: US – ESG-12

D. SUBSURFACE: GE – CINCGERFLEET

E. LAND: US – USMC 2-23

F. OPFOR: UK – HMS SUTHERLAND

G. LOGISTICS: US – ESG-2

H. COMMUNICATIONS/OPSEC: US AND GERMANY – ESG-2 AND CINCGERFLEET

I. MCM: UK – MCM HQ

J. AMPHIB: US – LSD/LPD (TBD)

WORKING GROUP LEAD WILL PROVIDE DIRECTION AND OVERSIGHT.

9. SCHEDULE OF EVENTS FOR BALTOPS 2005 IPC FOLLOWS:

6 DECEMBER (MONDAY)

TRAVEL DAY FOR ALL PARTICIPANTS

----

7 DECEMBER (TUESDAY)

0730-0815 CHECK-IN SHERATON CONFERENCE ROOM

0815 OPENING REMARKS BY ESG-12 AND INTRODUCTION

0830 CONFERENCE ADMIN/OVERVIEW

0840 COUNTRY/FORCE REPRESENTATIVE INTRODUCTIONS

0920 REVIEW CDC NOTES (C6F)/REVIEW IPC OBJECTIVES AND REQUIREMENTS

1000 PRESENTATION OF COMMAND AND CONTROL, WORKING GROUP ASSIGNMENTS AND OPORDER RESPONSIBILITIES

1030 TACTICAL PLANNING BRIEF

1230 DRAFT INITIAL PLANNING ORDERS

1300 SERIAL BRIEF

1330 WORKING GROUP OBJECTIVES

1345-1500 WORKING GROUP MEETINGS

1500-1600 WORKING GROUP PROGRESS REPORTS

1800-2000 RECEPTION HOSTED BY ESG-12 (SHERATON) (DRESS: CASUAL)

----

8 DECEMBER (WEDNESDAY)

0800 DAY ONE REVIEW AND DAY TWO OBJECTIVES

0830 ROE OVERVIEW

0900 PROPOSED TASK FORCE ORGANIZATION

0930 WORKING GROUP MEETINGS

1500-1530 WORKING GROUP PROGRESS REPORTS

----

9 DECEMBER (THURSDAY)

0800 DAY TWO REVIEW AND DAY THREE OBJECTIVES

0815 WORKING GROUP MEETINGS

1000 WORKING GROUP OUTBRIEFS

1400 IPC OBJECTIVES STATUS REVIEW

```
1430 ROADMAP, MPC AGENDA/LOGISTICS
1500 IPC WRAP-UP
---------
10 DECEMBER (FRIDAY)
TRAVEL DAY FOR ALL PARTICIPANTS
10. ADMINISTRATION.
   A. WEBSITE ACCESS: COMMANDS DESIGNATE 2-3 PERSONNEL TO OBTAIN
ACCESS TO THE HOA IN THE PARTNERS FOR PEACE INFORMATION
MANAGEMENT SYSTEM (PIMS) WEBSITE. THE FIRST STEP IS TO REGISTER AND
OBTAIN AN ACCOUNT AND PASSWORD. TO REGISTER GO TO THE FOLLOWING
SITE: HTTP: (DOUBLE SLASH) WWW.CONSORTIUM.PIMS.ORG
IN THE REMARKS SECTION.  ONCE YOU HAVE OBTAINED AN ACCOUNT GO TO THE
PIMS HOME PAGE AND SELECT BALTOPS UNDER THE ANNOUNCEMENT BANNER
(PASSWORD PROTECTED).  THIS IS WHERE ALL PERTINENT DOCUMENTS
RELATING TO HOA SOTHERN WATCH WILL BE POSTED.
   B. CONFERENCE. ROOM WILL BE EQUIPPED TO SUPPORT MICROSOFT
POWERPOINT BRIEFS WITH A PROJECTOR.  ESG-2 OPERATES POWERPOINT
2003.  COMMANDS PROVIDING POWERPOINT BRIEFS, EMAIL BRIEFS TO ESG-2
POC NLT 20 NOV.  MAX FILE ATTACHMENT SIZE IS 5MB.  FILE MAY BE
MAILED TO POC AT:
        CDR OMAR DENZEL
        COMMANDER EXPEDITIONARY STRIKE GROUP TWO
        UNIT 123456
        FPO AE 09506-4704
   C.  SHERATON WATERSIDE HOTEL
      (1) SHERATON PHUKET HOTEL PHUKET, THAILAND.  RESERVATIONS CAN BE
MADE DIRECT TO THE HOTEL AT 011-757-622-6664. FAX NUMBER IS
011-757-635-8271.  WEBSITE IS WWW.PHUKET.COM/SHERATON/.
FORTY (40) ROOMS ARE SET ASIDE FOR THE CONFERENCE.  ROOM CHARGE IS ONE
HUNDRED AND TEN (110) US PER NIGHT PLUS APPLICABLE TAXES AND FEES.
      (2) REQUEST THAT &quot;SOUTHERN WATCH PFP&quot; IS REFERENCED WHEN
BOOKING
RESERVATIONS.  TO ENSURE ADEQUATE AVAILABILITY, ATTENDEES ARE
ENCOURAGED TO MAKE RESERVATIONS NO LATER THAN 12 NOV 2004.
      (3) A CONFERENCE FEE OF TEN (10) US DOLLARS WILL BE COLLECTED
DURING CHECK-IN TUESDAY MORNING 7 DEC TO COVER ADMINISTRATIVE COSTS.
   D. FOR TRANSPORTATION ISSUES PLEASE CONTACT THE ESG-2 STAFF
DUTY OFFICER AT 757-642-6970. ADDITIONALLY, IF ANY ISSUES ARE
ENCOUNTERED WITH THE HOTEL, PLEASE CONTACT THE ESG-2 LOGISTICS
OFFICER AT 757-946-1234.
   F. INFORMATION ON THE PHUKET, THAILAND AREA MAY BE FOUND
ON THE WEB AT WWW.PHUKET.COM.
   G. ATTIRE.  THE CONFERENCE WILL BE CONDUCTED IN WORKING UNIFORM.
   H. POINTS OF CONTACT:
      C6F-CNE: LT JOSE DELGADOE –N37, DSN: 314-235-4022, COMM:
0044-207-514-4022, CELL: 0044-773-986-2216, FAX: 0044-207-514-4637,
EMAIL: JOSE.DELGADOE@NAVEUR.NAVY.MIL
      ESG-2: CDR OMAR DENZEL – N34, DSN 312-445-9595. COMM:
001-757-445-9595, CELL: 001-757-621-6352, FAX: 001-757-445-8703,
EMAIL:OMAR.DENZEL@NAVY.MIL</free_text>
  </general_text_information>
</mtf:general_administration_message>
```

Whether an organization steams independently, as part of a strike action group, or convoy, there must be some pre-established means to maintain communications. This is performed via an Operational Tasking Communications message via a tool known as Afloat Electromagnetic Spectrum Operations Program (AESOP).

G. ACP-126 USMTF OPTASK COMMS

```
UNCLASSIFIED
OPER/ALLIED PROTECTOR//
MSGID/GENADMIN/CTF 151/-/MAY//
SUBJ/OPTASK COMMS FOR CTF 151 ISO ALLIED PROTECTOR//
REF/A/MSGID:GENADMIN/CTF 151/231645ZJAN2004//
REF/B/MSGID:GENADMIN/CTF 151/181945ZFEB2005//
REF/C/MSGID:GENADMIN/CTF 151/251246ZMAR2005//
REF/D/MSGID:GENADMIN/CTF 151/271646ZAPR2005//
NARR/REF A IS CTF 151 OPTASK COMMS ISO ALLIED PROTECTOR. REF B IS
CHG 1
TO CTF 151 OPTASK COMMS OPERATION OCEAN SHIELD PART ONE. REF C IS
CHG 1 TO
//
POC/RIVERA/ITCS/CTF 151/LOC:HMS EDINBURGH/TEL:011 885-1250
/EMAIL:RIVERAS(AT)EDINBURGH.RNS.SMIL.MIL//
POC/KRENSHAW/IT2/CTF 151/LOC:HMS EDINBURG/TEL:021-259-2468
/EMAIL:KANESHIGEI(AT)EDINBURG.RNS.SMIL.MIL//
AKNLDG/YES//
GENTEXT/REMARKS/NOTE: THIS IS A NOTIONAL COMMS PLAN WITH FICTITIOUS
DATA FOR THE PURPOSE OF SHOWING PROOF OF CONCEPT FOR THE THESIS
ENTITLED DOCUMENT AND MESSAGE CENTRIC SECURITY USING XML
AUTHNTICATION AND ENCRYPTION FOR COALITION AND INTERAGENCY OPERATIONS
//
RMKS/NECOS: ANZ
#CTF 151_MDU_COORD/PURPOSE: CMD AND CONTROL OF TLAM OPS AND
EXERCISES.
PARTICIPANTS: TLAM UNITS
GUARD: AS REQUIRED
NECOS: ANZ
#CTF 151_COMM_COORD/PURPOSE: COORDINATION AND TROUBLESHOOTING FOR
COMMUNICATIONS PERSONNEL.
PARTICIPANTS: COMM CENTERS
GUARD: CONTINUOUS
NECOS: ANZ
---
CH101/SAMETIME/SIPR SERVER 205.0.XXX.XX
ROOMS:
#CTF 151_CMD/PURPOSE: COMMAND, CONTROL AND SITUATIONAL AWARENESS FOR
PRIMARY WATCH OFFICERS.
PARTICIPANTS: FLAG TAO AND TAO'S
GUARD: CONTINUOUS
NECOS: EDI
#CTF 151_SCC_COORD/PURPOSE: COORD SURFACE SHIPS
GUARD: CONTINUOUS
NECOS: WSC
#CTF 151_FOTC_COORD/PURPOSE: TRACK MANAGEMENT.
PARTICIPANTS: ALL FOTC DATA BASE MANAGERS
GUARD: CONTINUOUS
NECOS: EDI
```

```
#CTF 151_IWC_COORD/PURPOSE: COORD OF IWC.
PARTICIPANTS: HQ, IWC, ALL SHIPS EW MODULES, AND OTHER IWC SOURCES.
GUARD: AS REQUIRED
NECOS: EDI
#CTF 151_COMM_COORD/PURPOSE: COORDINATION AND TROUBLESHOOTING FOR
COMMUNICATIONS PERSONNEL.
PARTICIPANTS: COMM CENTERS
GUARD: CONTINUOUS
NECOS: EDI
------------------------------------------------------------------
D1/BCST/IAW NATIONAL RQMTS.
D2/SHIP-SHORE IAW NATIONAL RQMTS
  /1/ALL UNITS SUBMIT COMM GUARD SHIFT AS REQUIRED.  IN THE EVENT OF
     OUTAGE, NECOS/ALT NECOS WILL RELAY MESSAGE TRAFFIC FROM
     SERVICING COMMUNICATION CENTER.
E1/COMM GUARD/CIRCUIT GUARD REQUIREMENTS ARE PROMULGATED BY
   COMMANDERS IN THEIR DAILY INTENTIONS MESSAGES.
  /1/ST800A/BALTOPS CMD NET/UFO-9 CH-22/412.245/344.105-5K0G7W/
     AMST 152/W ALL CAPABLE UNITS COMMANDERS GUARD.
F1/EHF/SEE EHF SERVICE PLAN/PROMULGATED SEPCOR.
G1/TFCOMMS/AS LISTED IN CTF 151 CIRCUITS AND COMMAND NETS SECTIONS
   ABOVE.
G2/TFBDCST/ALL SHIPS AT A MINIMUM GUARD MMCC/MOCC
I1/1/CALLSIGN/COVERED CIRCUITS, USE SHIP NAMES (LESS U-S-S, U-S-N-S,
     OR SIMILAR PREFIX).
  /2/UNCOVERED CKTS: JANAP 119 CALLSIGNS. SHIPS WILL USE THEIR
     ASSIGNED JANAP 119 CALLSIGN FOR ALL CLEAR RADIO COMMUNICATIONS.
  /3/AIRCRAFT WILL USE JANAP 119 SQUADRON CALL SIGNS SUFFIXED BY
     AIRCRAFT SIDE NUMBER.
  /4/SECURE VOICE CALLSIGNS, COMMAND TITLES OR CWC WARFARE CALLSIGNS
     WILL BE USED ON SECURE VOICE NETS.  ENCRYPTED CALL SIGN
     USE IS PROHIBITED ON SECURE NETS.
  /5/SHIPS WILL USE INTERNATIONAL CALLSIGNS ON ORDERWIRES, NETTED
     DATA CIRCUITS AND SHIP/SHORE NETS.
I2/CODING/REFER TO REF H DAILY COMM STATUS XX2301ZMONYR.
I3/RECPOL
  /1/AUTHENTICATION IS REQUIRED ON ALL NON-SECURE CIRCUITS WHEN
     TRANSMITTING IN THE BLIND, ENTERING AND RE-ENTERING INTO THE
     NET AND PASSING FREQUENCY SHIFTS.  ZULU TIME WILL BE USED FOR
     IMPLEMENTING NEW TABLES FOR DETERMINING AUTHENTICATION.
J1/VSPOL/
  /1/MAXIMUM USE OF VISUAL COMMS WHENEVER POSSIBLE TO ENHANCE
     COMMS DISCIPLINE CONCERNING REDUCTION OF RECORD TRAFFIC AND
     GAIN MAXIMUM TRAINING OPPORTUNITIES FOR QUARTERMASTERS.  USE
     FILTERS AND CONICAL ADAPTERS ON SIGNAL SEARCH LIGHTS BETWEEN
     SUNSET AND SUNRISE.
K1/REPINST/
  /1/ENSURE CTG 151.O1 AND HMS EDINGURG ARE TO BE INCLUDED AS INFO
     ADDEES ON ALL COMMUNICATIONS RELATED MESSAGES.
  /2/CANVAS FLAGSHIPS/AND SHIPS IN COMPANY FOR MISSING NRS, CCS
     (EDINBURG) WILL SUBMIT BSR TO NCTAMS EURCENT.
  /3/FAST REACTION EXERCISES:  EDI WILL RESPOND FOR CTG 151.O1 ON ALL
     EMERGENCY ACTION RESPONSE TESTS.  CTU WILL RESPOND
     ACCORDINGLY FOR THEIR OWN EAMS; HOWEVER, ANZ MAY BE USED TO
     RELAY WHEN NECESSARY.
  /4/COMSPOT REPORTS SUBMITTED TO ANZ AND APPROPRIATE NCTAMS; INFO
     CTF 151 AND CTG 151.O1 WITHIN THIRTY MINUTES OF OUTAGE. USS
     BATTAAN WILL BE INFO ON ALL COMSPOTS AS ALT CCS.
Y1/SPECINST/1/EHF CAPABLE UNITS:
  /1/EHF TERMINAL ID NUMBER:
```

UNIT	TERMINAL ID	UNIT	TERMINAL ID
NCTAMS LANT	2222	NCTAMS EURCENT	2555, 2666
ANZIO	2333	NAKASAKI	2777

TORTUGA	2444	PAULEEN	2888
BATTAAN	1589		

Y1/SPECINST/2/APPLICABLE TO ALL:

/1/CALL SIGNS WILL BE SET IN THE FOLLOWING ORDER:

CTX	CALL SIGN	COLLECTIVE
CTF 151	VIPER	FLAMINGO
CTG 151.01	GRANT	KUMATE
CTG 151.02	JACKAL	JADE
CTG 151.04	FANNIE	SNAKE
CTG 151.07	MISMO	PIE
CTU 151.01.01	ASTRO	SNATCH
CTU 151.01.02	PIPER	BUSH
CTU 151.01.03	CUTIE	REAGAN
CTU 151.01.04	PUMA	ANKLE
CTU 151.01.05	TROJAN	KNEE
CTU 151.01.06	ROOK	LION
CTU 151.07.01	BISHOP	KNIGHT
CTU 151.07.02	AXEMAN	QUEEN

/2/TRIGRAPH INFORMATION FOR ALL UNITS:

UNIT	TRIGRAPH
ANZIO	ANZ
PAULEEN	PAL
TORTUGA	TOR
MCFAUL	MCF
HMS EDINBURG	EDI
HDMS PETER TORDENSKIOLD	PTO
RFS NASTOYCHIVIY	NAS
HDMS NIELS JUEL	NIJ
HSWMS NORRKOPING	NOR
HSWMS SPEJAREN	SPJ
FGS HAMBURG	HAM
FNS KOTKA	KOT
HSWMS KAPAREN	KAP
LVNS LODE	LOD
HMS LEEDS CASTLE	LEE
HMS BANGOR	BAN
HMS CATTISTOCK	CAT
FGS DATTELN	DAT
ORP GOPLO	GOP
HMS GRIMSBY	GRI
HMS LEDBURY	LED
ORP SNIARDWY	SNI
HDMS STOEREN	STO
ENS VAINDLO	VAI
FGS U-24	U24
ORP SOKOL	SOK
ORP POZNAN	POZ
RFS KALINIGRAD	KAL
USNS BIGHORN	BHN
SS PFC EUGENE A OBREGON	EAO
MV PFC DEWAYNE T WILLIAMS	DTW
HSWMS VISBORG	VIS
HMS SUTHERLAND	SUT
ORP KASZUB	KAS
FGS HABICHT	HAB
HSWMS TIRFING	TIR
HSWMS YSTAD	YST
LNS ZEMAITIS	ZEM

/3/EACH CTU WILL CREATE THEIR OWN SUPPLEMENTAL OPTASK COMMS AS NECESSARY. INFO CTF 151 ON ALL MESSAGES.

/4/ALL SHIPS MONITOR CHANNEL 16 FOR SAFETY.

/5/IAW REF O, HMS EDINBURG MAINTAINS THE SATHICOM GUARD FOR ALL UNITS IN COMPANY.

/6/COMMUNICATORS AND WATCHSTANDERS SHOULD IMMEDIATELY CHECK SATELLITE EQUIPMENT ONCE ANY ANOMALY IS DETECTED/SUSPECTED/ REPORTED. ENSURE ADHERENCE TO SATCOM POWER REGULATIONS COMMENSURATE WITH RELIABLE COMMS. REVIEW QUALITY MONITORING POLICIES.

/7/OPERATE WSC-3 SATCOM DAMA RADIOS IN FDX MODE. I.E., TWO WSC-3 TCVRS PER TD-1271, ONE AS A TRANSMIT AND ONE AS A RCV. CONFIGURE XMT WSC IN OFFSET 6 FOR ALL AND APPROPRIATE OFFSET FOR RCV WSC.

/8/ALL UNITS REVIEW REF H, DAILY COMM STATUS, FOR ANY CHANGES IN BCST OR MED SATELLITE CONFIGURATIONS.

/9/ALL UNITS USE MINIMUM POWER COMMENSURATE WITH RELIABLE COMMS.

/10/CUDIXS, FSM, AND SHF-PCMT TERMINATION ASSIGNMENTS IAW REF N. UNITS SUBMIT COMSHIFTS FOR DURATION OF TERM. IMMEDIATE RESTORAL WILL BE MMCC.

/11/ALL ATOS DURING BALTOPS 2005 WILL BE UNCLASSIFIED ONLY. ATO DISTRO PRIORITIES ARE:

A. PC NET
B. PIMS

/12/COALITION CIRCUITS WILL ALWAYS BE RESTORED FIRST. NOT ALL UNITS GUARD/PARTICIPATE IN ALL NETS. INDIVIDUAL UNIT COMMANDERS WILL DEVELOP RESTORATION PRIORITIES FOR THEIR UNIQUE CIRCUITS.

/13/MAXIMUM USE OF ZEN WILL REDUCE MESSAGE BACKLOGS. ENSURE THAT MESSAGES ADDRESSED TO CTF 151 UNITS AND COMMANDS ASHORE USE OPERATING SIGNAL "ZEN" AS APPROPRIATE IN FORMAT LINES 7 AND 8, AND ARE PASSED TO GROUP SAIL UNITS VIA SIPRNET EMAIL USING RADIO(AT)SHIP.DOMAIN.NAVY.SMIL.MIL ACCOUNTS OR THE APPROPRIATE SHIP'S NATO INITIAL DATA TRANSFER SYSTEM (NIDTS) EMAIL ACCOUNT.

/14/MONITORING: NAVY TACTICAL COMMUNICATIONS CIRCUITS ARE SUBJECT TO COMSEC MONITORING AND THE USE OF THESE CIRCUITS CONSTITUTES CONSENT TO MONITORING.

/15/GINGERBREAD PROCEDURES WILL BE REVIEWED AND EXECUTED WHEN EXPERIENCING INTRUSION ON CKTS.

/16/COMSEC AWARENESS IS A MUST IN DEGRADED COMM ENVIRONMENT. PROPER R/T PROCEDURES ARE ESSENTIAL. REVIEW RUTH PROCEDURES. TACTICAL COMM CKTS SUBJ TO COMSEC MONITORING UNDER C2 PROTECT PROGRAM. USE OF CKTS CONSTITUTES CONSENT TO MONITORING.

/17/CMD NETS ARE CONSIDERED TO BE DIRECTED. (CWC NECOS).
WARFARE CMDRS ARE FREE TO USE THESE CIRCUITS WHEN DEALING WITH THE BWC AND OTHER WARFARE CDRS. WARFARE COMMANDERS AND OTHER UNITS USE DESIGNATED WARFARE NETS WHEN REQUESTING AND/OR RECEIVING OPERATIONAL REPORTS FROM SHIPS/UNITS.

/18/ALL UNITS EQUIPPED WITH HAVEQUICK SHOULD USE IT TO THE MAXIMUM EXTENT POSSIBLE FOR AIRCRAFT CONTROL.

/19/NIDTS CAN BE USED TO EXCHANGE EMAIL BETWEEN NIDTS CAPABLE UNITS. UNITS WITH NIDTS ARE REQUIRED TO POST THEIR NIDTS EMAIL ADDRESSES TO THE COMMS POC SECTION OF PIMS SITE BY 25MAY05. (SEND TO CTF 66 TO HAVE POSTED).

/20/CRYPTO REQUIRMENTS:

**FOR SECURITY CONCERNS THIS SECTION INTENTIONALLY LEFT BLANK **

/21/ALL UNITS REPORT RFI PROBLEMS TO CTF 151INFO COMSIXTHFLT AND COMSECONDFLT. CTF 151 WILL DETERMINE AND ASSIGN REPLACEMENT FREQUENCIES AS REQUIRED.//

H. COE CMP XML REPRESENTATION OF OPTASK COMMS

```
<?xml version="1.0"?>
<mtf:general_administration_message
xmlns:mtf="urn:mtf:mil:usmtf:2004"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<operation_identification_data>
    <operation_codeword>ALLIED PROTECTOR</operation_codeword>
  </operation_identification_data>
  <message_identification>

<message_text_format_identifier>GENADMIN</message_text_format_identifier
>
    <originator>CTF 151</originator>
    <month_name>MAY</month_name>
  </message_identification>
  <subject>
    <message_subject>OPTASK COMMS FOR CTF 151 ISO ALLIED
PROTECTOR</message_subject>
  </subject>
  <reference>
    <serial_identifier>A</serial_identifier>
    <type_of_reference>

<message_text_format_identifier>GENADMIN</message_text_format_identifier
>
    </type_of_reference>
    <originator>CTF 151</originator>
    <date_and_or_time_of_reference>
      <reference_date_time_group>
        <day>23</day>
        <hour_time>16</hour_time>
        <minute_time>45</minute_time>
        <time_zone>Z</time_zone>
        <month_name>JAN</month_name>
        <year>2004</year>
      </reference_date_time_group>
    </date_and_or_time_of_reference>
  </reference>
  <reference>
    <serial_identifier>B</serial_identifier>
    <type_of_reference>

<message_text_format_identifier>GENADMIN</message_text_format_identifier
>
    </type_of_reference>
    <originator>CTF 151</originator>
    <date_and_or_time_of_reference>
      <reference_date_time_group>
        <day>18</day>
        <hour_time>19</hour_time>
        <minute_time>45</minute_time>
        <time_zone>Z</time_zone>
        <month_name>FEB</month_name>
        <year>2005</year>
      </reference_date_time_group>
    </date_and_or_time_of_reference>
  </reference>
  <reference>
    <serial_identifier>C</serial_identifier>
    <type_of_reference>

<message_text_format_identifier>GENADMIN</message_text_format_identifier
>
    </type_of_reference>
    <originator>CTF 151</originator>
    <date_and_or_time_of_reference>
      <reference_date_time_group>
        <day>25</day>
        <hour_time>12</hour_time>
        <minute_time>46</minute_time>
        <time_zone>Z</time_zone>
        <month_name>MAR</month_name>
        <year>2005</year>
      </reference_date_time_group>
    </date_and_or_time_of_reference>
  </reference>
  <reference>
    <narrative_information>
      <free_text xml:space = 'preserve'>REF A IS CTF 151 OPTASK COMMS
ISO ALLIED PROTECTOR. REF B IS
CHG 1
TO CTF 151 OPTASK COMMS OPERATION OCEAN SHIELD PART ONE. REF C IS
CHG 1 TO
</free_text>
    </narrative_information>
    <serial_identifier>D</serial_identifier>
    <type_of_reference>

<message_text_format_identifier>GENADMIN</message_text_format_identifier
>
    </type_of_reference>
    <originator>CTF 151</originator>
    <date_and_or_time_of_reference>
      <reference_date_time_group>
        <day>27</day>
        <hour_time>16</hour_time>
        <minute_time>46</minute_time>
        <time_zone>Z</time_zone>
        <month_name>APR</month_name>
        <year>2005</year>
      </reference_date_time_group>
    </date_and_or_time_of_reference>
  </reference>
  <point_of_contact_information>
    <contact_name>RIVERA</contact_name>
    <rank_or_position>ITCS</rank_or_position>
    <unit_identifier_or_call_sign>
      <unit_identifier>CTF 151</unit_identifier>
    </unit_identifier_or_call_sign>
    <poc_location>
      <location_name>HMS EDINBURGH</location_name>
    </poc_location>
    <group_of_fields>
      <telephone_number_or_frequency>
        <nonsecure_telephone_number>011 885-
1250</nonsecure_telephone_number>
      </telephone_number_or_frequency>
    </group_of_fields>
    <group_of_fields>
      <telephone_number_or_frequency>

<electronic_mail_address>RIVERAS(AT)EDINBURGH.RNS.SMIL.MIL</electronic_m
```

```
ail_address>
      </telephone_number_or_frequency>
    </group_of_fields>
  </point_of_contact_information>
  <point_of_contact_information>
    <contact_name>KRENSHAW</contact_name>
    <rank_or_position>IT2</rank_or_position>
    <unit_identifier_or_call_sign>
      <unit_identifier>CTF 151</unit_identifier>
    </unit_identifier_or_call_sign>
    <poc_location>
      <location_name>HMS EDINBURG</location_name>
    </poc_location>
    <group_of_fields>
      <telephone_number_or_frequency>
        <nonsecure_telephone_number>021-259-
2468</nonsecure_telephone_number>
      </telephone_number_or_frequency>
    </group_of_fields>
    <group_of_fields>
      <telephone_number_or_frequency>

<electronic_mail_address>KANESHIGEI(AT)EDINBURG.RNS.SMIL.MIL</electronic
_mail_address>
      </telephone_number_or_frequency>
    </group_of_fields>
  </point_of_contact_information>
  <acknowledgement_requirement>

<acknowledgement_requirement_indicator>YES</acknowledgement_requirement_
indicator>
  </acknowledgement_requirement>
  <general_text_information>
    <gentext_text_indicator>REMARKS</gentext_text_indicator>
    <free_text xml:space ='preserve'>NOTE: THIS IS A NOTIONAL COMMS PLAN
WITH FICTITIOUS
DATA FOR THE PURPOSE OF SHOWING PROOF OF CONCEPT FOR THE THESIS
ENTITLED DOCUMENT AND MESSAGE CENTRIC SECURITY USING XML
AUTHNTICATION AND ENCRYPTION FOR COALITION AND INTERAGENCY
OPERATIONS</free_text>
  </general_text_information>
  <remarks>
    <free_text xml:space = 'preserve'>NECOS: ANZ
#CTF 151_MDU_COORD/PURPOSE: CMD AND CONTROL OF TLAM OPS AND
EXERCISES.
PARTICIPANTS: TLAM UNITS
GUARD: AS REQUIRED
NECOS: ANZ
#CTF 151_COMM_COORD/PURPOSE: COORDINATION AND TROUBLESHOOTING FOR
COMMUNICATIONS PERSONNEL.
PARTICIPANTS: COMM CENTERS
GUARD: CONTINUOUS
NECOS: ANZ
---
CH101/SAMETIME/SIPR SERVER 205.0.XXX.XX
ROOMS:
#CTF 151_CMD/PURPOSE: COMMAND, CONTROL AND SITUATIONAL AWARENESS FOR
PRIMARY WATCH OFFICERS.
PARTICIPANTS: FLAG TAO AND TAO&apos;S
GUARD: CONTINUOUS
NECOS: EDI
#CTF 151_SCC_COORD/PURPOSE: COORD SURFACE SHIPS
GUARD: CONTINUOUS
```

```
NECOS: WSC
#CTF 151_FOTC_COORD/PURPOSE: TRACK MANAGEMENT.
PARTICIPANTS: ALL FOTC DATA BASE MANAGERS
GUARD: CONTINUOUS
NECOS: EDI
#CTF 151_IWC_COORD/PURPOSE: COORD OF IWC.
PARTICIPANTS: HQ, IWC, ALL SHIPS EW MODULES, AND OTHER IWC SOURCES.
GUARD: AS REQUIRED
NECOS: EDI
#CTF 151_COMM_COORD/PURPOSE: COORDINATION AND TROUBLESHOOTING FOR
COMMUNICATIONS PERSONNEL.
PARTICIPANTS: COMM CENTERS
GUARD: CONTINUOUS
NECOS: EDI
------------------------------------------------------------------
D1/BCST/IAW NATIONAL RQMTS.
D2/SHIP-SHORE IAW NATIONAL RQMTS
  /1/ALL UNITS SUBMIT COMM GUARD SHIFT AS REQUIRED.  IN THE EVENT OF
     OUTAGE, NECOS/ALT NECOS WILL RELAY MESSAGE TRAFFIC FROM
     SERVICING COMMUNICATION CENTER.
E1/COMM GUARD/CIRCUIT GUARD REQUIREMENTS ARE PROMULGATED BY
   COMMANDERS IN THEIR DAILY INTENTIONS MESSAGES.
  /1/ST800A/BALTOPS CMD NET/UFO-9 CH-22/412.245/344.105-5K0G7W/
     AMST 152/W ALL CAPABLE UNITS COMMANDERS GUARD.
F1/EHF/SEE EHF SERVICE PLAN/PROMULGATED SEPCOR.
G1/TFCOMMS/AS LISTED IN CTF 151 CIRCUITS AND COMMAND NETS SECTIONS
   ABOVE.
G2/TFBDCST/ALL SHIPS AT A MINIMUM GUARD MMCC/MOCC
I1/1/CALLSIGN/COVERED CIRCUITS, USE SHIP NAMES (LESS U-S-S, U-S-N-S,
     OR SIMILAR PREFIX).
  /2/UNCOVERED CKTS: JANAP 119 CALLSIGNS. SHIPS WILL USE THEIR
     ASSIGNED JANAP 119 CALLSIGN FOR ALL CLEAR RADIO COMMUNICATIONS.
  /3/AIRCRAFT WILL USE JANAP 119 SQUADRON CALL SIGNS SUFFIXED BY
     AIRCRAFT SIDE NUMBER.
  /4/SECURE VOICE CALLSIGNS, COMMAND TITLES OR CWC WARFARE CALLSIGNS
     WILL BE USED ON SECURE VOICE NETS.  ENCRYPTED CALL SIGN
     USE IS PROHIBITED ON SECURE NETS.
  /5/SHIPS WILL USE INTERNATIONAL CALLSIGNS ON ORDERWIRES, NETTED
     DATA CIRCUITS AND SHIP/SHORE NETS.
I2/CODING/REFER TO REF H DAILY COMM STATUS XX2301ZMONYR.
I3/RECPOL
  /1/AUTHENTICATION IS REQUIRED ON ALL NON-SECURE CIRCUITS WHEN
     TRANSMITTING IN THE BLIND, ENTERING AND RE-ENTERING INTO THE
     NET AND PASSING FREQUENCY SHIFTS.  ZULU TIME WILL BE USED FOR
     IMPLEMENTING NEW TABLES FOR DETERMINING AUTHENTICATION.
J1/VSPOL/
  /1/MAXIMUM USE OF VISUAL COMMS WHENEVER POSSIBLE TO ENHANCE
     COMMS DISCIPLINE CONCERNING REDUCTION OF RECORD TRAFFIC AND
     GAIN MAXIMUM TRAINING OPPORTUNITIES FOR QUARTERMASTERS.  USE
     FILTERS AND CONICAL ADAPTERS ON SIGNAL SEARCH LIGHTS BETWEEN
     SUNSET AND SUNRISE.
K1/REPINST/
  /1/ENSURE CTG 151.O1 AND HMS EDINGURG ARE TO BE INCLUDED AS INFO
     ADDEES ON ALL COMMUNICATIONS RELATED MESSAGES.
  /2/CANVAS FLAGSHIPS/AND SHIPS IN COMPANY FOR MISSING NRS, CCS
     (EDINBURG) WILL SUBMIT BSR TO NCTAMS EURCENT.
  /3/FAST REACTION EXERCISES:  EDI WILL RESPOND FOR CTG 151.O1 ON ALL
     EMERGENCY ACTION RESPONSE TESTS.  CTU WILL RESPOND
     ACCORDINGLY FOR THEIR OWN EAMS; HOWEVER, ANZ MAY BE USED TO
     RELAY WHEN NECESSARY.
  /4/COMSPOT REPORTS SUBMITTED TO ANZ AND APPROPRIATE NCTAMS; INFO
     CTF 151 AND CTG 151.O1 WITHIN THIRTY MINUTES OF OUTAGE. USS
     BATTAAN WILL BE INFO ON ALL COMSPOTS AS ALT CCS.
```

Y1/SPECINST/1/EHF CAPABLE UNITS:
/1/EHF TERMINAL ID NUMBER:

UNIT	TERMINAL ID	UNIT	TERMINAL ID
NCTAMS LANT	2222	NCTAMS EURCENT	2555, 2666
ANZIO	2333	NAKASAKI	2777
TORTUGA	2444	PAULEEN	2888
BATTAAN	1589		

Y1/SPECINST/2/APPLICABLE TO ALL:
/1/CALL SIGNS WILL BE SET IN THE FOLLOWING ORDER:

CTX	CALL SIGN	COLLECTIVE
CTF 151	VIPER	FLAMINGO
CTG 151.01	GRANT	KUMATE
CTG 151.02	JACKAL	JADE
CTG 151.04	FANNIE	SNAKE
CTG 151.07	MISMO	PIE
CTU 151.01.01	ASTRO	SNATCH
CTU 151.01.02	PIPER	BUSH
CTU 151.01.03	CUTIE	REAGAN
CTU 151.01.04	PUMA	ANKLE
CTU 151.01.05	TROJAN	KNEE
CTU 151.01.06	ROOK	LION
CTU 151.07.01	BISHOP	KNIGHT
CTU 151.07.02	AXEMAN	QUEEN

/2/TRIGRAPH INFORMATION FOR ALL UNITS:

UNIT	TRIGRAPH
ANZIO	ANZ
PAULEEN	PAL
TORTUGA	TOR
MCFAUL	MCF
HMS EDINBURG	EDI
HDMS PETER TORDENSKIOLD	PTO
RFS NASTOYCHIVIY	NAS
HDMS NIELS JUEL	NIJ
HSWMS NORRKOPING	NOR
HSWMS SPEJAREN	SPJ
FGS HAMBURG	HAM
FNS KOTKA	KOT
HSWMS KAPAREN	KAP
LVNS LODE	LOD
HMS LEEDS CASTLE	LEE
HMS BANGOR	BAN
HMS CATTISTOCK	CAT
FGS DATTELN	DAT
ORP GOPLO	GOP
HMS GRIMSBY	GRI
HMS LEDBURY	LED
ORP SNIARDWY	SNI
HDMS STOEREN	STO
ENS VAINDLO	VAI
FGS U-24	U24
ORP SOKOL	SOK
ORP POZNAN	POZ
RFS KALINIGRAD	KAL
USNS BIGHORN	BHN
SS PFC EUGENE A OBREGON	EAO
MV PFC DEWAYNE T WILLIAMS	DTW
HSWMS VISBORG	VIS
HMS SUTHERLAND	SUT
ORP KASZUB	KAS
FGS HABICHT	HAB
HSWMS TIRFING	TIR
HSWMS YSTAD	YST
LNS ZEMAITIS	ZEM

/3/EACH CTU WILL CREATE THEIR OWN SUPPLEMENTAL OPTASK COMMS AS NECESSARY. INFO CTF 151 ON ALL MESSAGES.

/4/ALL SHIPS MONITOR CHANNEL 16 FOR SAFETY.

/5/IAW REF O, HMS EDINBURG MAINTAINS THE SATHICOM GUARD FOR ALL UNITS IN COMPANY.

/6/COMMUNICATORS AND WATCHSTANDERS SHOULD IMMEDIATELY CHECK SATELLITE EQUIPMENT ONCE ANY ANOMALY IS DETECTED/SUSPECTED/ REPORTED. ENSURE ADHERENCE TO SATCOM POWER REGULATIONS COMMENSURATE WITH RELIABLE COMMS. REVIEW QUALITY MONITORING POLICIES.

/7/OPERATE WSC-3 SATCOM DAMA RADIOS IN FDX MODE. I.E., TWO WSC-3 TCVRS PER TD-1271, ONE AS A TRANSMIT AND ONE AS A RCV. CONFIGURE XMT WSC IN OFFSET 6 FOR ALL AND APPROPRIATE OFFSET FOR RCV WSC.

/8/ALL UNITS REVIEW REF H, DAILY COMM STATUS, FOR ANY CHANGES IN BCST OR MED SATELLITE CONFIGURATIONS.

/9/ALL UNITS USE MINIMUM POWER COMMENSURATE WITH RELIABLE COMMS.

/10/CUDIXS, FSM, AND SHF-PCMT TERMINATION ASSIGNMENTS IAW REF N. UNITS SUBMIT COMSHIFTS FOR DURATION OF TERM. IMMEDIATE RESTORAL WILL BE MMCC.

/11/ALL ATOS DURING BALTOPS 2005 WILL BE UNCLASSIFIED ONLY. ATO DISTRO PRIORITIES ARE:

A. PC NET
B. PIMS

/12/COALITION CIRCUITS WILL ALWAYS BE RESTORED FIRST. NOT ALL UNITS GUARD/PARTICIPATE IN ALL NETS. INDIVIDUAL UNIT COMMANDERS WILL DEVELOP RESTORATION PRIORITIES FOR THEIR UNIQUE CIRCUITS.

/13/MAXIMUM USE OF ZEN WILL REDUCE MESSAGE BACKLOGS. ENSURE THAT MESSAGES ADDRESSED TO CTF 151 UNITS AND COMMANDS ASHORE USE OPERATING SIGNAL &quot;ZEN&quot; AS APPROPRIATE IN FORMAT LINES 7 AND 8, AND ARE PASSED TO GROUP SAIL UNITS VIA SIPRNET EMAIL USING RADIO(AT)SHIP.DOMAIN.NAVY.SMIL.MIL ACCOUNTS OR THE APPROPRIATE SHIP&apos;S NATO INITIAL DATA TRANSFER SYSTEM (NIDTS) EMAIL ACCOUNT.

/14/MONITORING: NAVY TACTICAL COMMUNICATIONS CIRCUITS ARE SUBJECT TO COMSEC MONITORING AND THE USE OF THESE CIRCUITS CONSTITUTES CONSENT TO MONITORING.

/15/GINGERBREAD PROCEDURES WILL BE REVIEWED AND EXECUTED WHEN EXPERIENCING INTRUSION ON CKTS.

/16/COMSEC AWARENESS IS A MUST IN DEGRADED COMM ENVIRONMENT. PROPER R/T PROCEDURES ARE ESSENTIAL. REVIEW RUTH PROCEDURES. TACTICAL COMM CKTS SUBJ TO COMSEC MONITORING UNDER C2 PROTECT PROGRAM. USE OF CKTS CONSTITUTES CONSENT TO MONITORING.

/17/CMD NETS ARE CONSIDERED TO BE DIRECTED. (CWC NECOS). WARFARE CMDRS ARE FREE TO USE THESE CIRCUITS WHEN DEALING WITH THE BWC AND OTHER WARFARE CDRS. WARFARE COMMANDERS AND OTHER UNITS USE DESIGNATED WARFARE NETS WHEN REQUESTING AND/OR RECEIVING OPERATIONAL REPORTS FROM SHIPS/UNITS.

/18/ALL UNITS EQUIPPED WITH HAVEQUICK SHOULD USE IT TO THE MAXIMUM EXTENT POSSIBLE FOR AIRCRAFT CONTROL.

/19/NIDTS CAN BE USED TO EXCHANGE EMAIL BETWEEN NIDTS CAPABLE UNITS. UNITS WITH NIDTS ARE REQUIRED TO POST THEIR NIDTS EMAIL ADDRESSES TO THE COMMS POC SECTION OF PIMS SITE BY 25MAY05. (SEND TO CTF 66 TO HAVE POSTED).

/20/CRYPTO REQUIRMENTS:

** FOR SECURITY CONCERNS THIS SECTION INTENTIONALLY LEFT BLANK **

```
 /21/ALL UNITS REPORT RFI PROBLEMS TO CTF 151INFO COMSIXTHFLT AND
COMSECONDFLT.  CTF 151 WILL DETERMINE AND ASSIGN REPLACEMENT
FREQUENCIES AS REQUIRED.</free_text>
  </remarks>
</mtf:general_administration_message>
```

All things have a beginning and an end. As a participating organization's role in a mission draws to an end, the task force commander may deem it appropriate to send a farewell message stating the organizations contribution in relation to success of the overall mission objective and wishing the organization a safe transit back to their respective destination.

I. ACP-126 USMTF FAREWELL MESSAGE

```
UNCLASSIFIED
MSGID/GENADMIN/CCSG12/-/JUN//
SUBJ/ COALITION ANTIPIRACY OPERATIONS 2005 FAREWELL //
GENTEXT/REMARKS/1. PLEASE PASS TO CAPT PATROSKY,COMMANDING OFFICER,
ORP SIAPAN.  CAPTAIN PATROSKY, CONGRATULATIONS ON A MOST SUCCESSFUL
MISSION. THE CREW OF ORP SIAPAN IS COMMENDED FOR THEIR SUPERB
CONTRIBUTIONS AND PARTICIPATION DURING EACH PHASE OF THE PURSUIT.
THROUGHOUT THE EXECUTION PROCESS, THE DIRECT INVOLVEMENT OF SIAPAN
HELPED DETENTION OF SEVERAL PIRATE SUSPECTS THEREBY KEEPING THE
INTERNATIONAL SEA LINES OF COMMUNICATIONS FREE AND OPEN FOR WORLD
TRADE.
     OUR NATION LOOKS FORWARD TO CONTINUED COOPERATIONS BETWEEN OUR
TWO COUNTRIES IN EFFORTS OF PROMOTING PEACE AND LONGEVITY. AS YOU
DEPART KNOW THAT YOU DEMONSTRATED SUPERIOR EXPERTISE OPERATING 12
NATIONS, ACCOMPLISHED YOUR OWN NATIONAL OBJECTIVES AND DEVELOPED A
CAMARADERIE WITH NAVAL AND MARINE FORCES THAT ALSO ENJOY A RICH
MARITIME HERITAGE.
     HAVE A SAFE TRANSIT TO YOUR HOMEPORT FOR A WELL-DESERVED REUNION
WITH FAMILY AND FRIENDS. REAR ADMIRAL WILLIAMS SENDS.//
```

J. COMMON OPERATING ENVIRONMENT COMMON MESSAGE PROCESSOR (COE CMP) GENERATED XML REPRESENTATION OF FAREWELL MESSAGE

```xml
<?xml version="1.0"?>
<mtf:general_administration_message
    xmlns:mtf="urn:mtf:mil:usmtf:2004"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<message_identification>

<message_text_format_identifier>GENADMIN</message_text_format_identifier>
        <originator>CCSG12</originator>
        <month_name>JUN</month_name>
    </message_identification>
    <subject>
        <message_subject>COALITION ANTIPIRACY OPERATIONS 2005
FAREWELL</message_subject>
    </subject>
    <general_text_information>
        <gentext_text_indicator>REMARKS</gentext_text_indicator>
        <free_text xml:space ='preserve'>1. PLEASE PASS TO CAPT
PATROSKY,COMMANDING OFFICER,
            ORP SIAPAN.  CAPTAIN PATROSKY, CONGRATULATIONS ON A MOST SUCCESSFUL
            MISSION. THE CREW OF ORP SIAPAN IS COMMENDED FOR THEIR SUPERB
            CONTRIBUTIONS AND PARTICIPATION DURING EACH PHASE OF THE PURSUIT.
            THROUGHOUT THE EXECUTION PROCESS, THE DIRECT INVOLVEMENT OF SIAPAN
            HELPED DETENTION OF SEVERAL PIRATE SUSPECTS THEREBY KEEPING THE
            INTERNATIONAL SEA LINES OF COMMUNICATIONS FREE AND OPEN FOR WORLD
            TRADE.
            OUR NATION LOOKS FORWARD TO CONTINUED COOPERATIONS BETWEEN OUR
            TWO COUNTRIES IN EFFORTS OF PROMOTING PEACE AND LONGEVITY. AS YOU
            DEPART KNOW THAT YOU DEMONSTRATED SUPERIOR EXPERTISE OPERATING 12
            NATIONS, ACCOMPLISHED YOUR OWN NATIONAL OBJECTIVES AND DEVELOPED A
            CAMARADERIE WITH NAVAL AND MARINE FORCES THAT ALSO ENJOY A RICH
            MARITIME HERITAGE.
            HAVE A SAFE TRANSIT TO YOUR HOMEPORT FOR A WELL-DESERVED REUNION
            WITH FAMILY AND FRIENDS. REAR ADMIRAL WILLIAMS SENDS.</free_text>
    </general_text_information>
</mtf:general_administration_message>
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. TOP NATIONAL PRIORITIES OF 37 INTERNATIONAL MARITIME LEADERS

Proceedings magazine interviewed 37 maritime leaders and compiled their comments in respects to the critical issues that they saw in relations to their respective nations national interests (Proceedings 2009). From this article, a chart was constructed that enabled a comparison of the major issues across the 37 nations. Table 9 illustrates the key points that bind these nations together to form the basis of current and future cooperation against a common cause. Maintaining the Sea Lines of Communications, Preventing Piracy, and Enforcing the Economic Exclusive Zones were among the top issues. Other issues emphasized but were less common across the nation's collective critical interests were Terrorism, Drug/Human Trafficking, Environmental Disasters and Education of the public to guard against sea blindness.

Name	Title	Country	Sea Blindness/ Ignorance of the Sea	Terrorism	Piracy	Sea Lines of Communication	Environmental Disasters	Drug/ Human Trafficking	EEZ
ADM Jorge Omar	Chief of Staff, Argentine Navy	Argentinia				X			X
VADM R. H. Crane	Chief of Navy, Australia	Australia				X			
RADM Jean-Paul Robyns	Commander, Belgium Maritime Component	Belgium		X	X	X			
ADM Julio Soares de Moura Neto	Commandant, Brazilian Navy	Brazil				X	X	X	X
VADM Drew W. Robertson	Chief of Maritime Staff, Canadian Navy	Canada				X			
ADM Rodolfo Codina Diaz	Commander-in-Chief, Chilean Navy	Chile				X	X	X	X
ADM Almirante Guillermo Barrera Hurtado	Commander, Columbian Naval Forces	Columbia		X	X			X	
RADM Ante Urlic	Commander, Croatian Navy	Croatia				X			
RADM Nils Christian Wang	Admiral, Danish Fleet	Denmark		X	X	X	X		
COL Abdourahman Aden Cher	Commandant, Djibouti Navy	Dijbouti		X	X	X		X	X
VADM Julio Cesar Ventura Bayonet	Commander-in-Chief, Dominican Republic Navy	Dominican Republic		X				X	X
RADM Aland Molestina Malta	Chief of Staff, Ecuadoran Navy	Ecuador				X			X
LCDR J. J. Fox	Commander, Fiji Navy	Fiji							X
ADM Pierre-Francois Forissier	Chief of Staff, French Navy	France		X	X	X			
VADM Wolfgang E. Nolting	Chief of the German Navy Staff	Germany		X	X	X			
VADM Georgios Karamalikis	Commander-in-Chief, Hellenic Navy	Greece		X	X				
ADM Tedjo Edhy Purdijatno	Chief of Staff, Indonesian Navy	Indonesia			X	X	X	X	X
ADM Paolo La Rosa	Chief of the Italian	Italy			X	X			

	Navy General Staff								
ADM Keiji Akahosi	Chief of Staff, Japan Maritime Self Defense Force	Japan		X	X	X	X		X
MAJ GEN Dari Al Zaben	Commander, Royal Jordanian Naval Force	Jordan		X	X	X		X	
CAPT Aleksandrs Palvovics	Commander-in-Chief, Latvian Naval Forces	Latvia							
RADM Ali El Moallem	Commander, Lebanese Navy	Lebanon		X		X			
ADM Dato' Sri Abdul Aziz bib Hj Jaafar	Royal Malaysian Navy Chief	Malaysia				X			X
LT GEN Robertus Zuiderwijk	Commander, Royal Netherlands Navy	Netherland		X	X	X			
RADM David Ledson	Chief of Navy, New Zealand	New Zealand	X				X		X
RADM Juan Estrada Garcia	Chief Admiral, Nicaraguan Navy	Nicaragua						X	X
RADM Haakon Bruun-Hanssen	Chief of Staff, Royal Norwegian Navy	Norway				X			X
ADM Noman Bashir	Chief of the Naval Staff, Pakistan Navy	Pakistan			X	X	X	X	X
ADM Rolando Antonio Navarrete Salomon	Commander, Peruvian Navy	Peru			X	X		X	X
VADM Andrzej Karweta	Commander-in-Chief, Polish Navy	Poland		X		X			
ADM Fernando Jose Ribeiro de Melo Gomes	Chief of Naval Staff, Portuguese Navy	Portugal	X	X	X			X	X
VADM J. Mudimu	Chief, South African Navy	South Africa	X		X		X	X	X
ADM Manuel Rebollo	Chief of Staff, Spanish Navy	Spain			X	X			
RADM Anders Grenstad	Chief of Staff, Royal Swedish Navy	Sweden				X			
ADM Khamthorn Pumhiran	Commander-in-Chief, Royal Thai Navy	Thialand		X	X		X	X	X
RADM Ahmed M. Al Sabab Al Tenaiji	Commander United Arab Emirates Naval Forces	United Arab Emirates		X	X	X	X	X	X
Admiral Sir Jonathon Band	First Sea Lord and Chief of Navy Staff,	United Kingdom	X						

	Royal Navy								
			4	16	19	26	10	14	19
			10.81%	**43.24%**	**51.35 %**	**70.27%**	**27.03%**	**37.84%**	**51.35 %**
Sea lines of communication (abbreviated as **SLOC**) is a term describing the primary maritime routes between ports, used for trade, logistics and naval forces.									
An **environmental disaster** is a disaster that is due to human activity and should not be confused with natural disasters.									
Exclusive Economic Zone (**EEZ**) is a seazone over which a state has special rights over the exploration and use of marine resources. It stretches from the edge of the state's territorial sea out to 200 nautical miles from its coast.									
Terrorism is the intentional use or threat to use violence against civilians and non-combatants "in order to achieve political goals"									
Sea Blindness is ignorance of the importance of the sea to everyday life.									
Piracy consists of any of the following acts: (a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State; (b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft; (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).									

Table 9. This table illustrates the national concerns of international maritime leaders around the world.

APPENDIX C. AVCL TO KML XSLT

Translations between XML-Based Languages are critical to establish an interoperable-networked operating environment in which the security is embedded directly into the document. By performing the translation and embedding security at the document level, the feeds may be available to any participating multinational or multiagency partner that possesses the appropriate credentials without the requirement to exchange cryptographic technology because the process is be based solely on the open standard technology that strictly adheres to the W3C specifications for digital signature and encryption.

The following XML is a XML Stylesheet that adapts XML written in autonomous Vehicle Command Languange (AVCL) to Keyhole Markup Language (KML)

A. XML-BASED AVCL TO KML TRANSLATIONS

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:fo="http://www.w3.org/1999/XSL/Format" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:fn="http://www.w3.org/2005/xpath-functions" xmlns="http://www.opengis.net/kml/2.2">

<!-- TODO:  author(s), creation date -->

  <xsl:output method="xml" indent="yes" exclude-result-prefixes="xsl fo xs fn"/>
    <xsl:template match="/">
        <kml>
            <Document>
                <xsl:apply-templates
select="AVCL/body/MissionResults/SampledResults"/>
            </Document>
        </kml>
    </xsl:template>
    <xsl:template match="SampledResults">
        <Placemark>
            <name>
                <xsl:text>Telemetry Point #</xsl:text>
                <xsl:value-of select="position()"/>
            </name>
            <xsl:if test="position()=1">
                <LookAt>
                    <longitude>
                        <xsl:value-of select="substring-
after(UUVTelemetry/GeographicPosition/@description,',')"/>
                    </longitude>
                    <latitude>
                        <xsl:value-of select="substring-
before(UUVTelemetry/GeographicPosition/@description,',')"/>
                    </latitude>
                    <altitude>1000</altitude>
                    <range>0</range>
                    <tilt>45</tilt>
                    <heading>0</heading>
                </LookAt>
            </xsl:if>
    <!-- to-do: TimeStamp generation logic needs testing
            <xsl:call-template name="generateTimeStamp"/> -->
            <styleURL>#msn_ylw-pushpin</styleURL>
            <Point>
                <coordinates>
                    <xsl:value-of select="format-number(number(substring-
after(UUVTelemetry/GeographicPosition/@description,',')),'#0.#####')"/>
                    <xsl:text>,</xsl:text>
                    <xsl:value-of select="format-number(number(substring-
before(UUVTelemetry/GeographicPosition/@description,',')),'#0.#####')"/>
                </coordinates>
            </Point>
        </Placemark>
    </xsl:template>
    <xsl:template name="generateTimeStamp">
        <TimeStamp>
            <when>
                <xsl:value-of select="../MissionStartTime/@year"/>
                <xsl:text>-</xsl:text>
                <xsl:call-template name="getMonthValue">
                    <xsl:with-param name="month"
select="../MissionStartTime/@month"/>
                </xsl:call-template>
                <xsl:text>-</xsl:text>
                <xsl:if test="../MissionStartTime/@day&lt;10">
                    <xsl:text>0</xsl:text>
                </xsl:if>
                <xsl:value-of select="../MissionStartTime/@day"/>
                <xsl:text>T</xsl:text>
                <xsl:variable name="seconds" select="UUVTelemetry/@timeStamp"/>
                <!-- compute the number of hours in the timestamp -->
                <xsl:variable name="hours" select="floor($seconds div 3600)"/>
                <!-- compute the number of seconds left over after computing the
number of hours in the timestamp -->
                <xsl:variable name="leftover" select="$seconds mod 3600"/>
                <xsl:if test="$hours &lt; 10">
                    <xsl:text>0</xsl:text>
                </xsl:if>
                <xsl:value-of select="number(../MissionStartTime/@hour)+$hours"/>
                <xsl:text>:</xsl:text>
                <xsl:variable name="minutes" select="floor($leftover div 60)"/>
                <xsl:if test="$minutes &lt; 10">
                    <xsl:text>0</xsl:text>
                </xsl:if>
                <xsl:value-of
```

```
select="number(../MissionStartTime/@minute)+$minutes"/>
                                <xsl:text>:</xsl:text>
                                <!-- compute the number of seconds left over after computing the
number of minutes left in the timestamp -->
                                <xsl:variable name="leftoverSeconds" select="$leftover mod 60"/>
                                <xsl:if test="$leftoverSeconds &lt; 10">
                                        <xsl:text>0</xsl:text>
                                </xsl:if>
                                <xsl:value-of
select="number(../MissionStartTime/@second)+$leftoverSeconds"/>
                                <xsl:text>Z</xsl:text>
                        </when>
                </TimeStamp>
        </xsl:template>
        <xsl:template name="getMonthValue">
                <xsl:param name="month"/>
                <xsl:choose>
                        <xsl:when test="month='January'">
                                <xsl:text>01</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='February'">
                                <xsl:text>02</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='March'">
                                <xsl:text>03</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='April'">
                                <xsl:text>04</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='May'">
                                <xsl:text>05</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='June'">
                                <xsl:text>06</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='July'">
                                <xsl:text>07</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='August'">
                                <xsl:text>08</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='September'">
                                <xsl:text>09</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='October'">
                                <xsl:text>10</xsl:text>
                        </xsl:when>
                        <xsl:when test="month='November'">
                                <xsl:text>11</xsl:text>
                        </xsl:when>
                        <xsl:otherwise>
                                <xsl:text>12</xsl:text>
                        </xsl:otherwise>
                </xsl:choose>
        </xsl:template>
</xsl:stylesheet>
```

B. XML-BASED DATA TO ADAPTED TO CUSTOMIZED OUTPUT

XML-based data can be adapted from one XML data format to another XML data format for processing in different systems. The XML data below was customized to suite the needs of KML. Once data is adapted to the new data format, it can be represented in a textually or graphicly. Figure 55 represents a graphical representation of the KML data as seen through GOOGLE Earth.

```
        <?xml version="1.0" encoding="UTF-8"?>
<kml xmlns="http://www.opengis.net/kml/2.2">
        <Placemark>
                <TimeStamp>
                        <Time>1970-12-01T00:35:49.7147139999997Z</Time>
                </TimeStamp>
                <Point>
                        <coordinates>-85.75543,30.12944</coordinates>
                </Point>
        </Placemark>
        <Placemark>
                <TimeStamp>
                        <Time>1970-12-01T00:35:50.6894590000002Z</Time>
                </TimeStamp>
                <Point>
                        <coordinates>-85.75543,30.12944</coordinates>
                </Point>
        </Placemark>
        <Placemark>
                <TimeStamp>
                        <Time>1970-12-01T00:35:51.718871Z</Time>
                </TimeStamp>
                <Point>
                        <coordinates>-85.75543,30.12944</coordinates>
                </Point>
        </Placemark>
        <Placemark>
                <TimeStamp>
                        <Time>1970-12-01T00:35:52.690979Z</Time>
                </TimeStamp>
                <Point>
                        <coordinates>-85.75543,30.12944</coordinates>
                </Point>
        </Placemark>
```

```
<Placemark>
        <TimeStamp>
                <Time>1970-12-01T00:35:53.710955Z</Time>
        </TimeStamp>
        <Point>
                <coordinates>-85.75543,30.12944</coordinates>
        </Point>
</Placemark>
<Placemark>
        <TimeStamp>
                <Time>1970-12-01T00:35:54.6767070000001Z</Time>
        </TimeStamp>
        <Point>
                <coordinates>-85.75543,30.12944</coordinates>
        </Point>
</Placemark>


<!—Additional data omitted -->


        <Placemark>
        <TimeStamp>
                <Time>1970-12-01T01:07:30.711753Z</Time>
        </TimeStamp>
        <Point>
                <coordinates>-85.75788,30.12671</coordinates>
        </Point>
</Placemark>
<Placemark>
        <TimeStamp>
                <Time>1970-12-01T01:07:31.6892710000002Z</Time>
        </TimeStamp>
        <Point>
                <coordinates>-85.75788,30.12672</coordinates>
        </Point>
</Placemark>
<Placemark>
        <TimeStamp>
                <Time>1970-12-01T01:07:32.7190879999998Z</Time>
        </TimeStamp>
        <Point>
                <coordinates>-85.75788,30.12672</coordinates>
        </Point>
</Placemark>
<Placemark>
```

```
                <TimeStamp>
                        <Time>1970-12-01T01:07:33.70559499999999Z</Time>
                </TimeStamp>
                <Point>
                        <coordinates>-85.75788,30.12673</coordinates>
                </Point>
        </Placemark>
</kml>
```

C. GRAPHICAL REPRESENTATION OF XML-BASED KML DATA

There are various tools available that can represent XML-based data visually. Open source tools such as X3D-Earth and GOOGLE Earth are a few tools that can adapt data to visual formats. Figure 55 illustrates KML data adapted to the GOOGLE Earth tool. Note that this image is included for demonstration purposes only. Google Earth licensing restricts the distribution of such imagery to personal use only unless otherwise licensed (http://www.google.com/intl/en-us/help/legalnotices_maps.html).

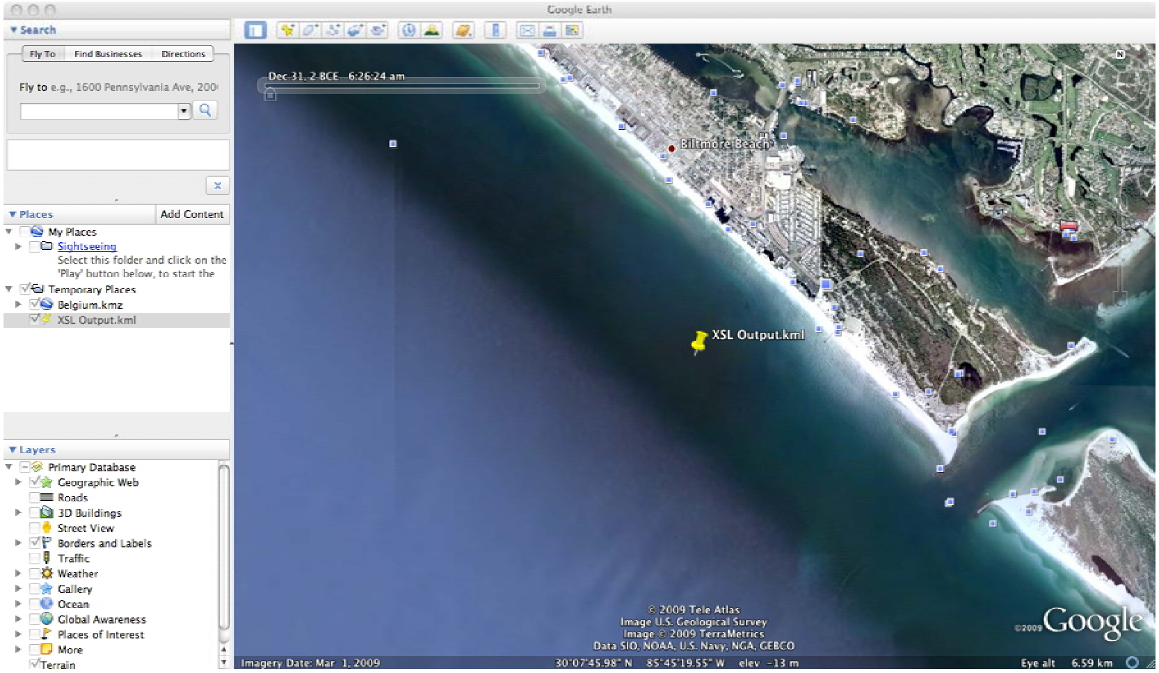


Figure 55. After the AVCL file is converted to KML it can be visualized in applications like Google Earth or other applications that accept KML output.

Web3D consortium members producing X3D-Earth implementations are currently planning to add support for KML on a royalty free basis. X3D-Earth project is a presents a viable means for the creation of a standards-based 3D visualization infrastructure for visualizing real-world object and information constructs in a geospatial context utilizing Web architecture, XML languages, and open protocols. Therefore, this is an appealing technology with much potential to support all personal and business-related activities. For additional information on X3D-Earth visit http://x3d-earth.nps.edu and http://www.web3d.org/x3d-earth.

APPENDIX D. SECURITY FEATURES OF X3D-EDIT

A robust toolset to generate graphics that can be digitally signed and encrypted with the most common methodologies has evolved significantly during the evolution of this thesis. Of note is the Extensible Three Dimensional (X3D) Graphic tool. It is an XML-based toolset for developing a vast array of 3D scenes and complex images, as can be scene throughout the Scenario Authoring and Visualization for Graphical Environments (SAVAGE) archive. X3D-Edit includes features to support XML Canonicalization, XML Digital Signature, XML Encryption and lossless compression tools to include EXI compression.

A. X3D-EDIT'S ROBUST ARRAY OF XML-BASED SECURITY FEATURES

"X3D-Edit is an open-source extensible three-dimensional (X3D) XML-based graphics file editor that enables simple error-free editing, authoring and validation of X3D or VRML scene-graph files. Context-sensitive tooltips provide concise summaries of each X3D node and attribute. More generally, it is an XML editor, customized to edit X3D scene graphs. It can be used to apply style sheet transformations to generate other file types, such as HTML and VRML97 (Web3D Consortium)" It is written in the JAVA programming language and is equipped with several plugins that support activities from chat to encryption of visual scenes. X3D-Edit is by design platform independent.

NPS Professor, Don Brutzman and his team of elite Java programmers to include Mike Bailey, Terry Norbratten, and Don McGregor currently support x3D-Edit. The project is based on open source standards-based XML technology as proposed by the World Wide Web Consortium Recommendations. Code contributions from other sources are reviewed and plugins made accessible if within the guidelines of the project. The SAVAGE team is currently working towards integrating an EXI implementation within the X3D-Edit code base.

X3D-Edit is equipped with a full array of tools to support XML-Well formed verification, XML validation via various methods, XML Canonicalization, XML digital signature, and XML Encryption. With the integration of Portecle, XML inate security features are enhanced to cover a broader array of open source encryption methodologies available for X3D-Edit. Portecle allows for the creation, managing, and examining of keystores, keys, certificates, certificate requests, certificate revocation lists and more.

B. X3D-EDIT SECURITY FEATURES

X3D-EDIT adheres to the base principles of XML

- XML Documents must be well-formed
- XML Documents must be valid
- Though optional XML Documents may specify a canonicalization (C14N) methodology. C14N is required for XML digital signature implementation.

Well-formness and validity checks are seemless performed seamlessly by the X3D-Edit after the addition or removal of each component from the X3D scene. Well-formedness and validity checks are must occur before any other operation in XML. In regards to XML digital signature, they are required. As seen in Figure 56 the flow of operations follows the XML digital signature specification.

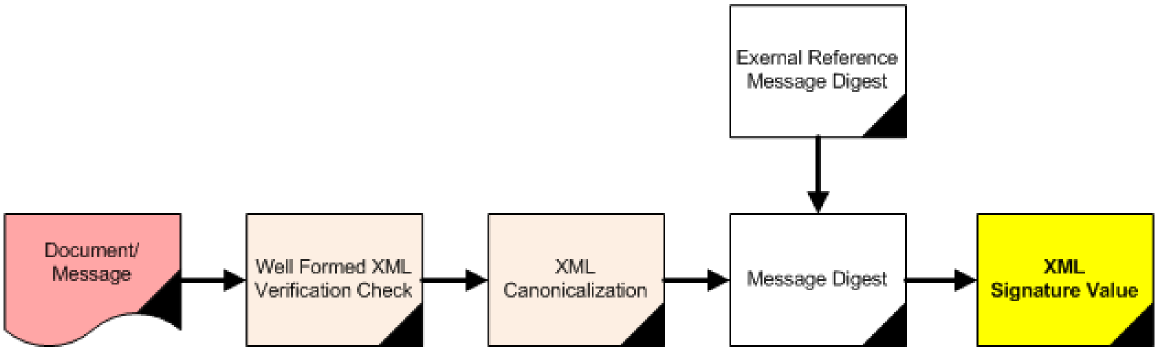
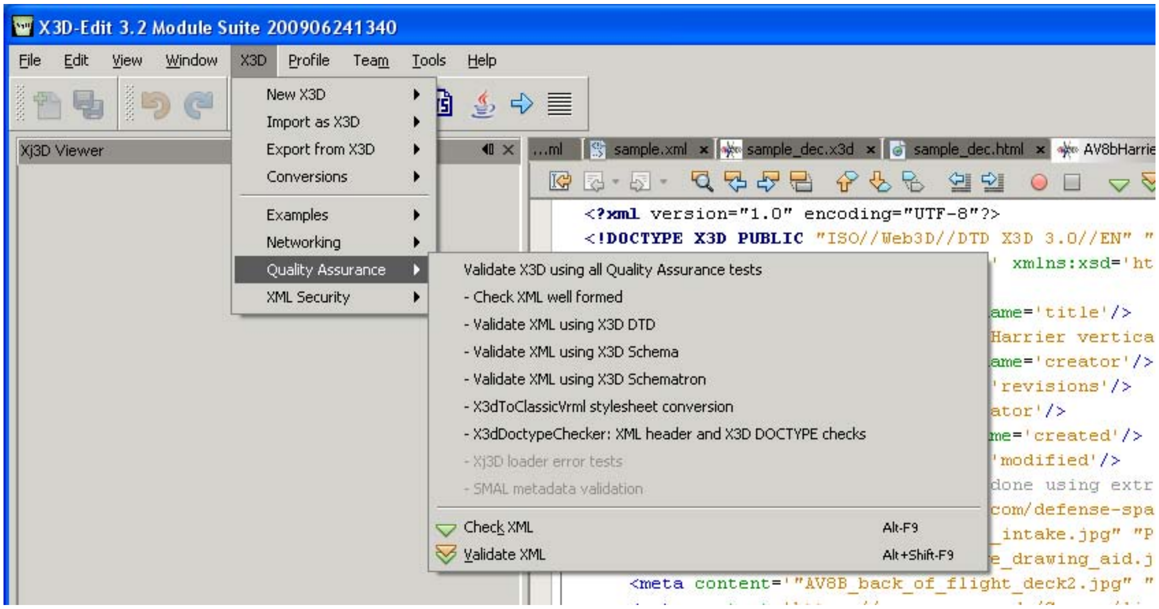


Figure 56. X3D-Edit follows the digital signature specification by ensuring that well formedness checks and validity checks are performed before any other operation.

X3D-Edit separates the operations under the X3D-Edit dropdown menu under the subtopic of "Quality Assurance." Under this topic the user can select to validate X3D-Edit using and X3D-Edit DTD, Schema, or Schematron, as well as a few others that are beyond the scope of this thesis. Figure 57 illustrates the X3D Quality Assurance menu and options available.


X3D-Edit 3.2 Module Suite 200906241340
File
Edit
View
Window
X3D
Profile
Team
Tools
Help
Xj3D Viewer
...ml
sample.xml
sample_dec.x3d
sample_dec.html
AV8bHarrie
New X3D
Import as X3D
Export from X3D
Conversions
Examples
Networking
Quality Assurance
XML Security
Validate X3D using all Quality Assurance tests
- Check XML well formed
- Validate XML using X3D DTD
- Validate XML using X3D Schema
- Validate XML using X3D Schematron
- X3dToClassicVrml stylesheet conversion
- X3dDoctypeChecker: XML header and X3D DOCTYPE checks
- Xj3D loader error tests
- SMAL metadata validation
Check XML Alt-F9
Validate XML Alt+Shift-F9

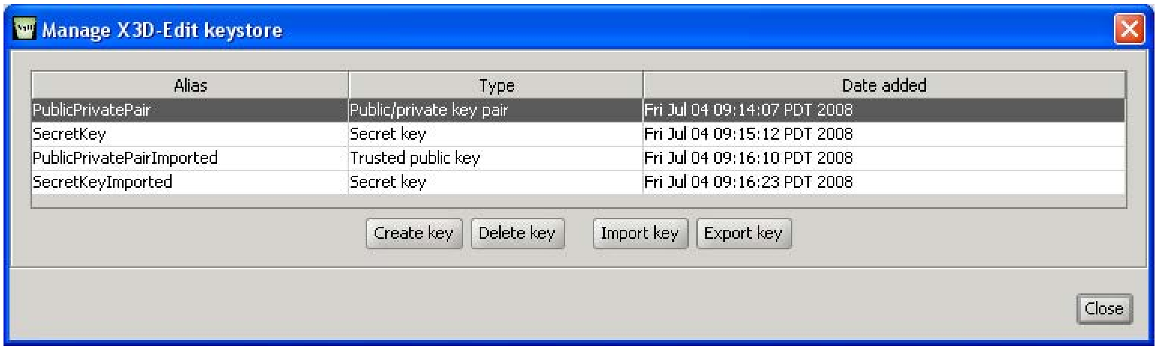
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.0//EN" "
' xmlns:xsd='ht
ame='title'/>
Harrier vertica
ame='creator'/>
'revisions'/>
ator'/>
me='created'/>
'modified'/>
done using extr
com/defense-spa
_intake.jpg" "P
e_drawing_aid.j
<meta content='"AV8B_back_of_flight_deck2.jpg" "
```

Figure 57. X3D-Edit offers a array of validations available for an X3D scene as well as various other tools. These features are essential to the proper validation of verifying that the document or scene generated is well formed and valid under the X3D schema.

Well-formedness and validity checks are the first stages of X3D-Edit under the XML digitatal signature specification. The XML Security menu illustrated in Figure 61 offers the other features to support XML digital signature and encryption. Of note are the Manage XML Security Keystore, which is a password protected site that maintains the digital certificates and for the user. The Manage XML security keystore option offers two methods of managing digital keys, which are via the innate X3D-Edit keystore that was originally built into the X3D-Edit tool or the Portecle, which is a third-party tool that was integrated within the X3D-Edit toolset. Portecle is discussed in further detail later in this section.

When the Manage XML Security Keystore option is selected, the user is prompted for a password. Upon successful acceptance of the entered password, the

Manage X3D-Edit keystore option dialog appears. This option allows the user to browse, create, delete, import, and export keys. The X3D-Edit keystore dialogue is illustrated in Figure 58.



Alias	Type	Date added
PublicPrivatePair	Public/private key pair	Fri Jul 04 09:14:07 PDT 2008
SecretKey	Secret key	Fri Jul 04 09:15:12 PDT 2008
PublicPrivatePairImported	Trusted public key	Fri Jul 04 09:16:10 PDT 2008
SecretKeyImported	Secret key	Fri Jul 04 09:16:23 PDT 2008

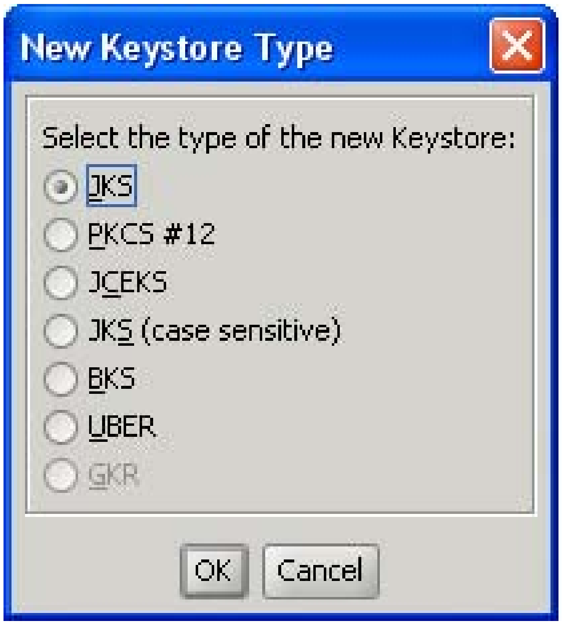
Figure 58. X3D-Edit allows the user to browse, create, delete, import, and export keys. These keys serve the basis of creating a digitally signed document in addition to encrpypting the document.

When a create key is selected, the user is given the opportunity to create either a Secret key for encrypting the document or a Public/Private key pair for signing the document. Using symmetric key encryption the entity receiving an encrypted document can open the decrypt the document. The key distribution problem is left up to each organizations security practicioners for implementation. The public/private key pair is for signing the document. The private key is neither shared nor made available to the general public. However, the public keys are distributed to those entities that the user seeks to converse securely. The create public/private key pair option is critical to assuring message integrity and sender authenticity.

When the manage keystore using Portecle option is selected another Portecle dialog box appears which allows the user list all keys in the user's keychain. Furthermore, Portecle provides a full suite of tools that allow greater functionality and a more diverse selection in the type of keys that the user can generate. Figure 59 illustrates all possible types of keystores that Portecle can generate. Portecle offers several types of keystores

- Java Key Store (JKS) which is Sun's Microsystems Keystore format
- Public Key Cryptography Standard (PKSC #12) which RSA's Personal Information Exchange Syntax Standard

- Java Cryptography Extension Keystore (JCEKS) which is a more secure form of JKS
- Bouncy Castle Keystore (BKS) which is Bouncy Castles version of JKS
- Bouncy Castle Uber Keystore (BKS) which is a more secure version of BKS
- GNU Keyring Keystore that requires a GNU Classpath version 9 or later installed.

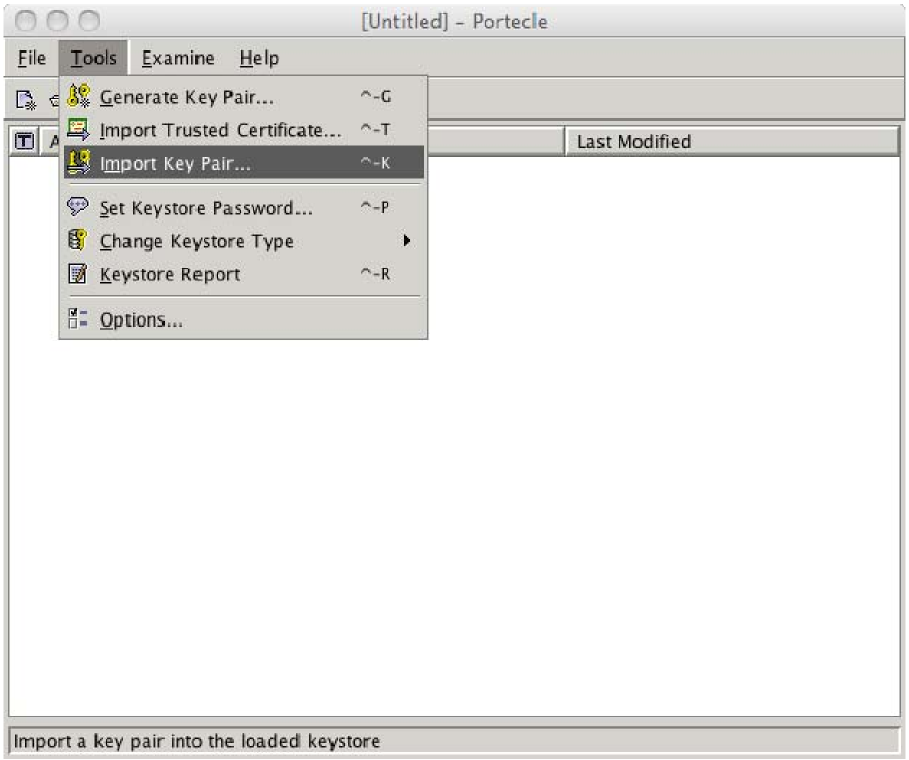


Select the type of the new Keystore:

● JKS
○ PKCS #12
○ JCEKS
○ JKS (case sensitive)
○ BKS
○ UBER
○ GKR

Figure 59. Portecle offers a variety of keystore types, which enhances capability across a variety of potential security soultions.

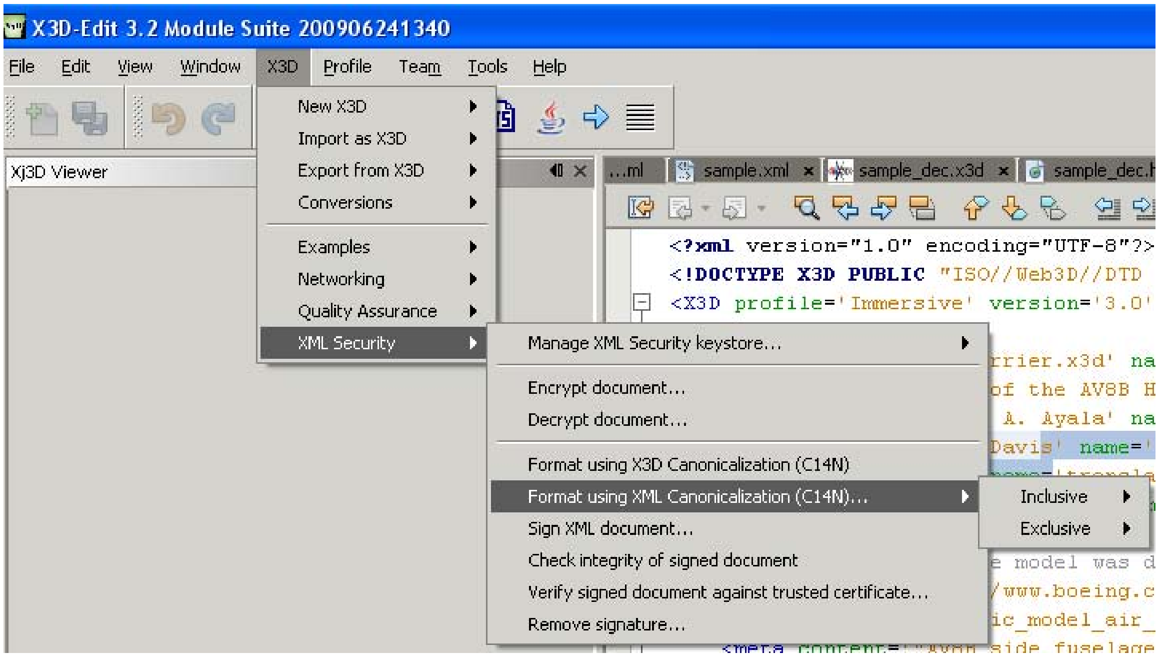
As with the default built in application, keys can either be created, deleted, imported, or exported. Keystore types can also be changed via the tools menu. Figure 59 illustrates an example of the Portecle tools that facilitates key generation, certificate and key pair import, as well as various administrative tasks such as keystore password and changing keystore type and also a report feature. The examine feature gives the user the ability to inspect the Certificate, the Certificate Revocation List (CRL), the actual transport layer security or security socket layer connection and the certificate requests itselft. Finally the the Help menu option provides both online and embedded documentation on the Portecle tool. For additional information on Portecle, visit http://portecle.sourceforge.net.



Import a key pair into the loaded keystore

Figure 60. Portecle tools grants a variety of selections inclusive of an option, which allows the user to select a certification authority (CA) certicificate keystore.

Canonicalization (C14N) is optional for most applications but a required feature for using the XML security. Within X3D-Edit it is accessed through the XML Security option of the X3D taskbar. There are two different types of X3D C14N, the XML Canonicalization which adheres strictly to the specification such as ensuring opening and closing tags exists for every element and the X3D C14N method that ensures operates in a more efficient manner to minimize file size and still comply within the guidelines of XML. Once such difference is for empty tags, such as <book> the X3D method places a slash at the end before the closing bracket such that it would appear like <book/>. The XML specification on the other hand would have the example displayed as <book></book> thereby having a closing tag for every open tag. In accordance with the W3C specification, the canonicalization method employed during digital signature is contained within the X3D/XML code.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD
<X3D profile='Immersive' version='3.0'
rrier.x3d' na
of the AV8B H
A. Ayala' na
Davis' name='
e model was d
/www.boeing.c
ic_model_air_
<meta content='AV8B side fuselage
```

Figure 61. X3D-Edit offers two methods of C14N, X3D and XML Canonicalization. Although the X3D C14N is based on the W3C specification there are areas where it may deviate. As a result it is highly recommended that the implementation used is negotiated with partners prior to deviating from the XML specification.

The remaining features of the security suite contained within X3D-Edit are self-explanatory. For example, for every signed document received there is a method of verifying the signature against trusted certificates and checking the signed document. There are also options for removing a signature. It is noted that once a document is signed, that any changes to the document invalidates the signature. Encryption and decryption of the document is also a option. Further information is available at the W3C Web site and also at https://savage.nps.edu/X3D-Edit.

Within the problem domain X3D-Edit effectively employs XML security to accomplish all of the prerequisite features of specificed in the XML security specification as illustrated in Figure 62. EXI compression is integrated into X3D-Edit. Through EXI compression implementation the best possible compression performance for XML-based data is achieved.

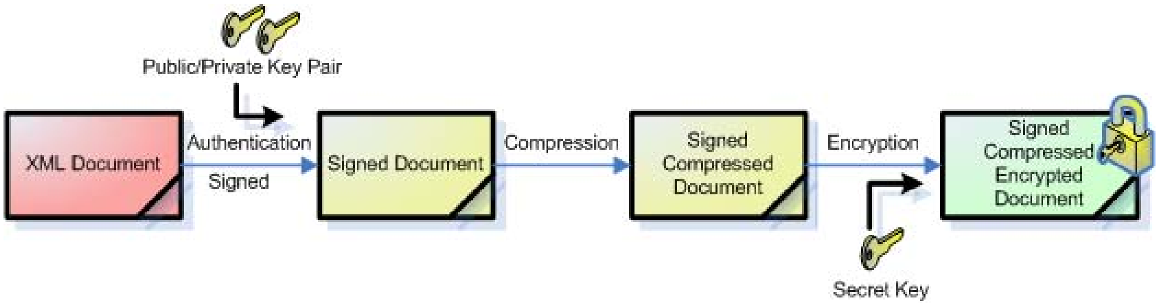


Figure 62. X3D-Edit complies with the W3C recommendation for XML digital signature and XML encryption. It signs and encrypts documents, as described within the W3C XML security specifications.

The World Wide Web Conosortium has an example of the full implementation the security features used within X3D edit. The URL to find the readme file is located at http://www.web3d.org/x3d/content/examples/Basic/Security/x3dSecurityReadMe.html

C. MODELING EXAMPLES BY X3D-EDIT

X3D-Edit produces an array of graphical user scenes that are available to the general public via the SAVAGE archive, X3DforWebAuthors site, and the W3C. A snapshot of a few of the examples that can be found at these sites are illustrated from Figure 63 through 65. Unique realistic 3D graphics are possible using this X3D Edit that also enables imports from different formats and exports to traditional VRML.

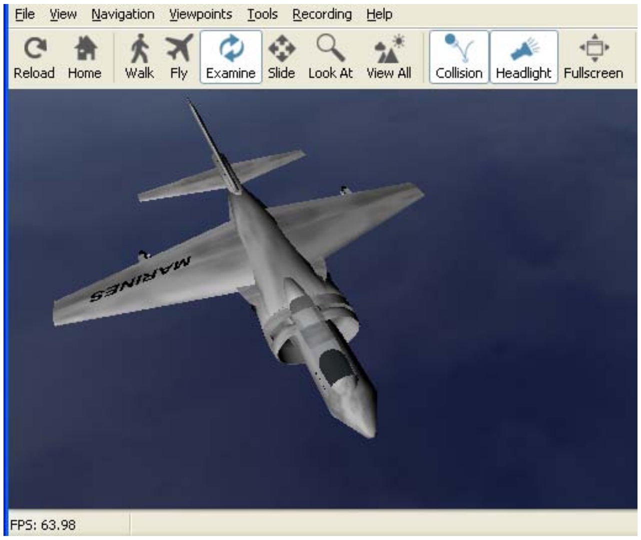


Figure 63. X3D-Edit authored model of a Marine Corp AV-8 Harrier in flight.

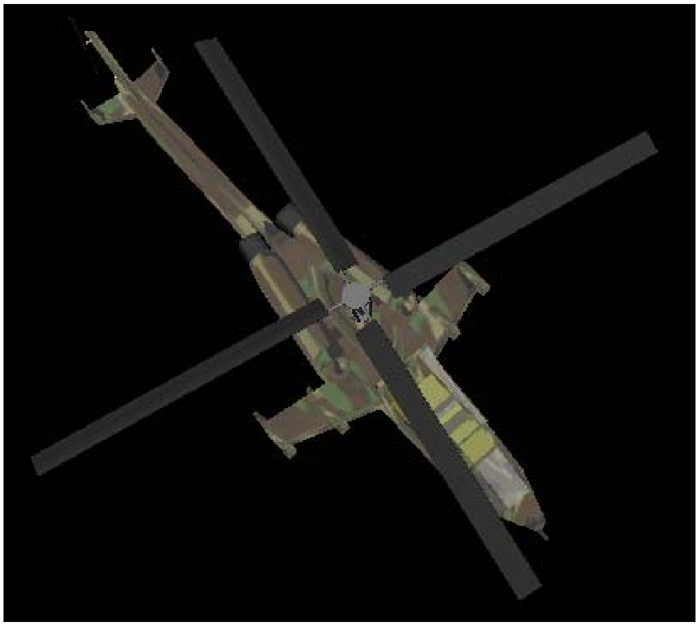


Figure 64. X3D-Edit authored model of a Marine Corp AH1 Super Cobra in flight that is displayed using the Octaga viewer within a web browser.

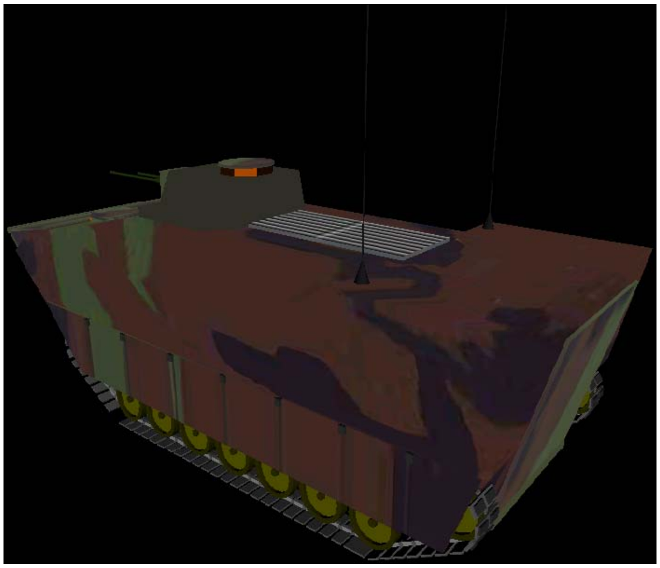


Figure 65. X3D-Edit authored model of a Marine Corp AAAV1 Amphious Assault Vehicle within a web browser window.

There are several images and full scenes created with X3D-Edit tool suite. The possibilities of the array of simulations that can be created using this tool are without bounds. A key point to remember about X3D-Edit is that it is an open source solution that carries the GNU licence, which means that it can be fully integrated with any product or used as a stand-alone tool at no charge to the distributer. However, any changes to the X3D-Edit code base must be freely available to the general public for review and integration into other products. This does not mean that a private organization cannot maintain proprietary technology. It simple means that they must ensure that their organizational secrets are not so integrated within the X3D code base that they cannot share the their changes to the X3D-Edit codebase (not integration technique) with the general public.

B. SUMMARY

X3D-Edit is a powerful graphics and scene visualization tool with several impressive security features that are in compliance with the W3C XML Canonicalization, XML Digital Signature, and XML Encryption recommendations. It checks for well formedness, validates against an array of X3D Schemas and DTDs, and facilitates not only signing but key generation and storage of an array of certificates via the keystore. With the integration of Portecle, the cryptographic feature set available in X3D-Edit are greatly enhanced. It is a definite contender for an all-in-one secure solution for authoring X3D graphics and scene graphs.

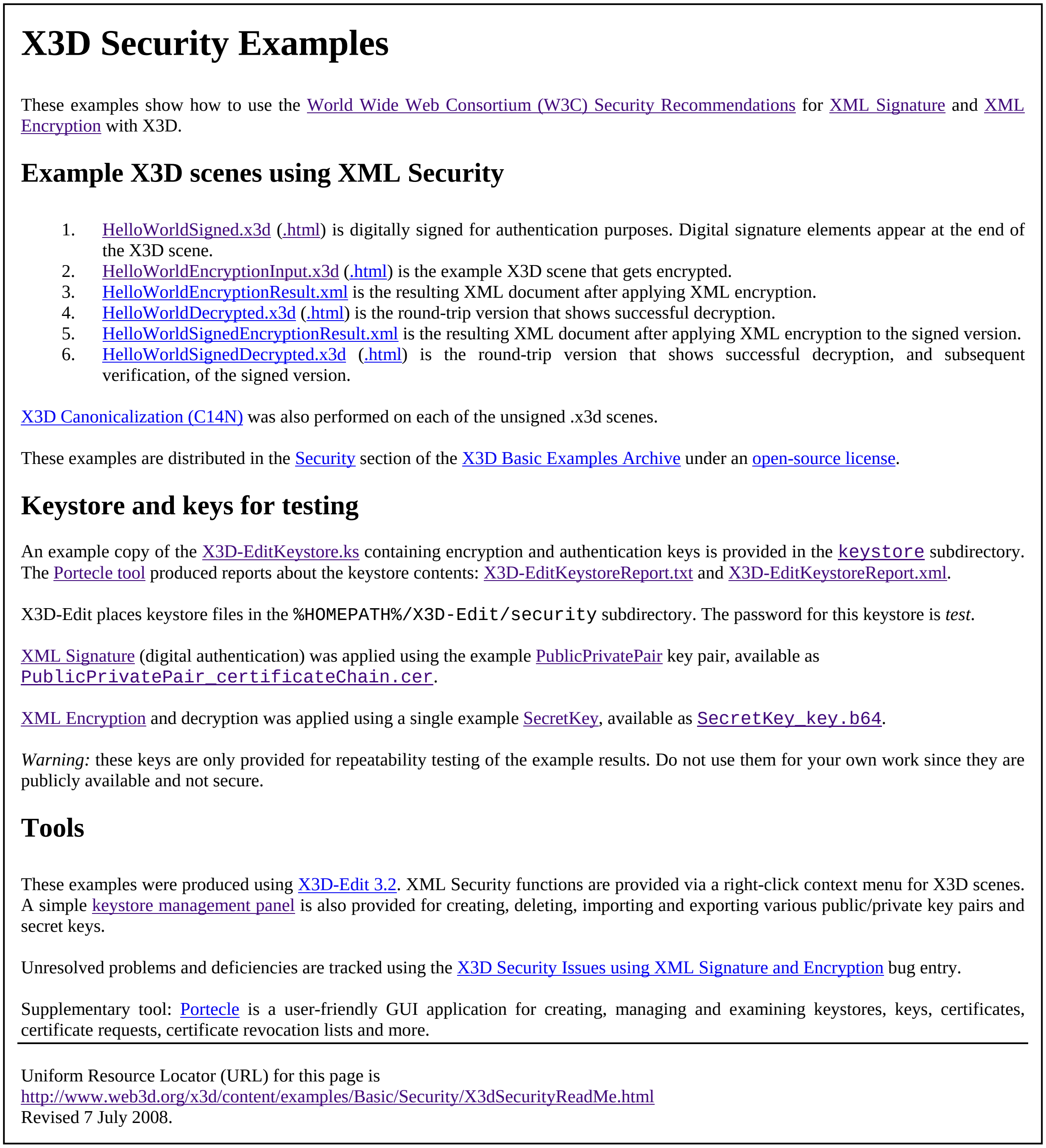
APPENDIX E. X3D SECURITY EXAMPLES

The SAVAGE Team implemented the World Wide Web Consortium specification for XML Canonicalization, XML Encryption and XML Digital Signature. Figures 66 and 67 illustrate webpages that support XML Security examples. The are located at the following sites:

http://www.web3d.org/x3d/content/examples/Basic/Security/X3dSecurityReadMe.html
http://www.web3d.org/x3d/content/examples/Basic/Security

Figures 68 through 71 illustrate XML that are undergoing the respective XML Security operations. Note, that all of these files underwent the C14N process prior to XML digital signature and XML Encryption. These figures represent the HelloWorld globe that was illustrated in Figure 16. It is significant to recognize that each both XML Encryption and XML Digital Signature increases the size of the original input file. However, after the decryption process restores the file.

A. X3D SECURITY EXAMPLES HTML PAGE



X3D Security Examples

These examples show how to use the World Wide Web Consortium (W3C) Security Recommendations for XML Signature and XML Encryption with X3D.

Example X3D scenes using XML Security

1. HelloWorldSigned.x3d (.html) is digitally signed for authentication purposes. Digital signature elements appear at the end of the X3D scene.
2. HelloWorldEncryptionInput.x3d (.html) is the example X3D scene that gets encrypted.
3. HelloWorldEncryptionResult.xml is the resulting XML document after applying XML encryption.
4. HelloWorldDecrypted.x3d (.html) is the round-trip version that shows successful decryption.
5. HelloWorldSignedEncryptionResult.xml is the resulting XML document after applying XML encryption to the signed version.
6. HelloWorldSignedDecrypted.x3d (.html) is the round-trip version that shows successful decryption, and subsequent verification, of the signed version.

X3D Canonicalization (C14N) was also performed on each of the unsigned .x3d scenes.

These examples are distributed in the Security section of the X3D Basic Examples Archive under an open-source license.

Keystore and keys for testing

An example copy of the X3D-EditKeystore.ks containing encryption and authentication keys is provided in the `keystore` subdirectory. The Portecle tool produced reports about the keystore contents: X3D-EditKeystoreReport.txt and X3D-EditKeystoreReport.xml.

X3D-Edit places keystore files in the `%HOMEPATH%/X3D-Edit/security` subdirectory. The password for this keystore is *test*.

XML Signature (digital authentication) was applied using the example PublicPrivatePair key pair, available as `PublicPrivatePair_certificateChain.cer`.

XML Encryption and decryption was applied using a single example SecretKey, available as `SecretKey_key.b64`.

Warning: these keys are only provided for repeatability testing of the example results. Do not use them for your own work since they are publicly available and not secure.

Tools

These examples were produced using X3D-Edit 3.2. XML Security functions are provided via a right-click context menu for X3D scenes. A simple keystore management panel is also provided for creating, deleting, importing and exporting various public/private key pairs and secret keys.

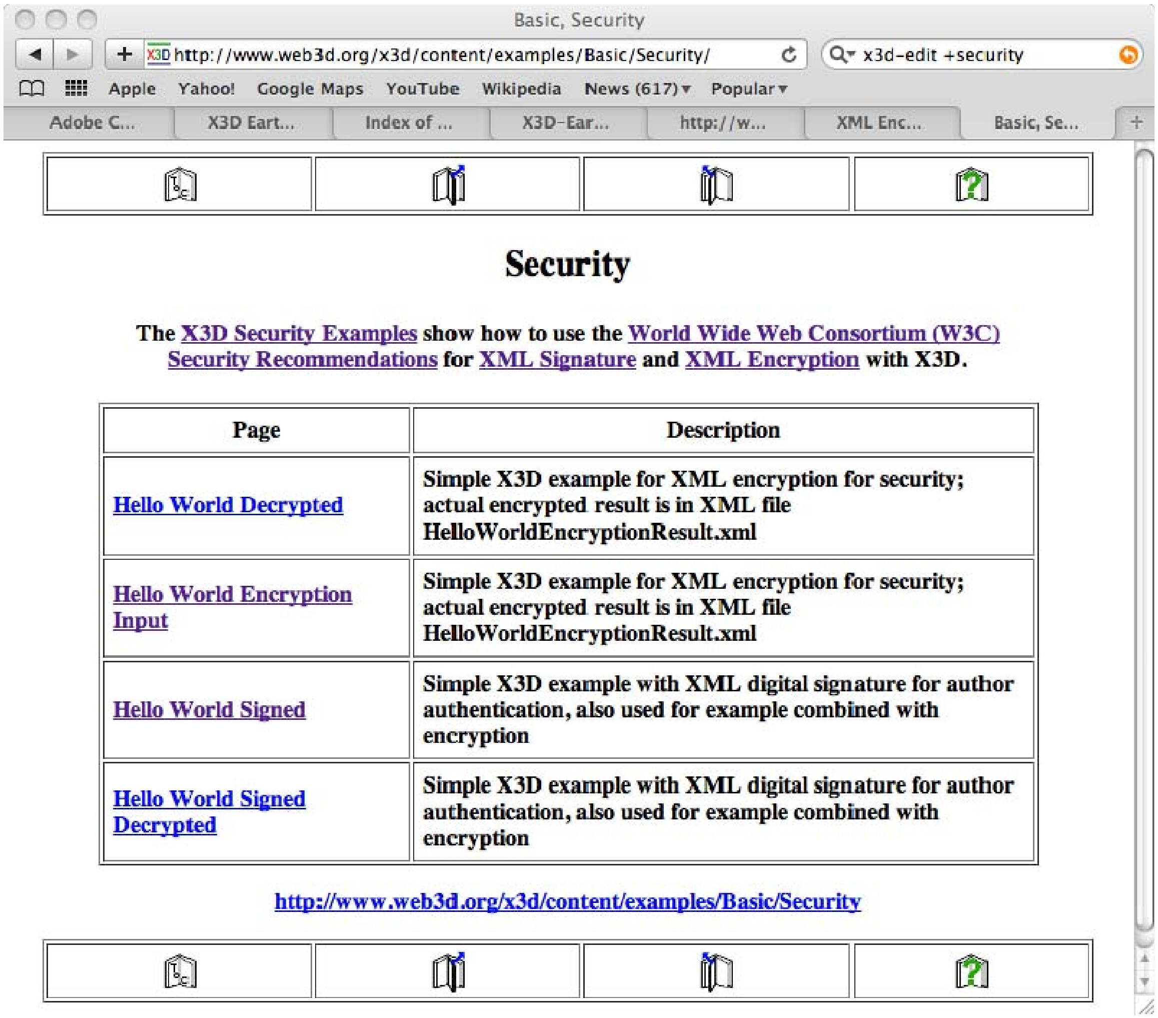
Unresolved problems and deficiencies are tracked using the X3D Security Issues using XML Signature and Encryption bug entry.

Supplementary tool: Portecle is a user-friendly GUI application for creating, managing and examining keystores, keys, certificates, certificate requests, certificate revocation lists and more.

Uniform Resource Locator (URL) for this page is
http://www.web3d.org/x3d/content/examples/Basic/Security/X3dSecurityReadMe.html
Revised 7 July 2008.

Figure 66. The W3C X3D Security examples site is helpful to authors to gain and understanding of the implementation of XML Security.

B. SECURITY DIRECTORY CATALOG PAGE



Security

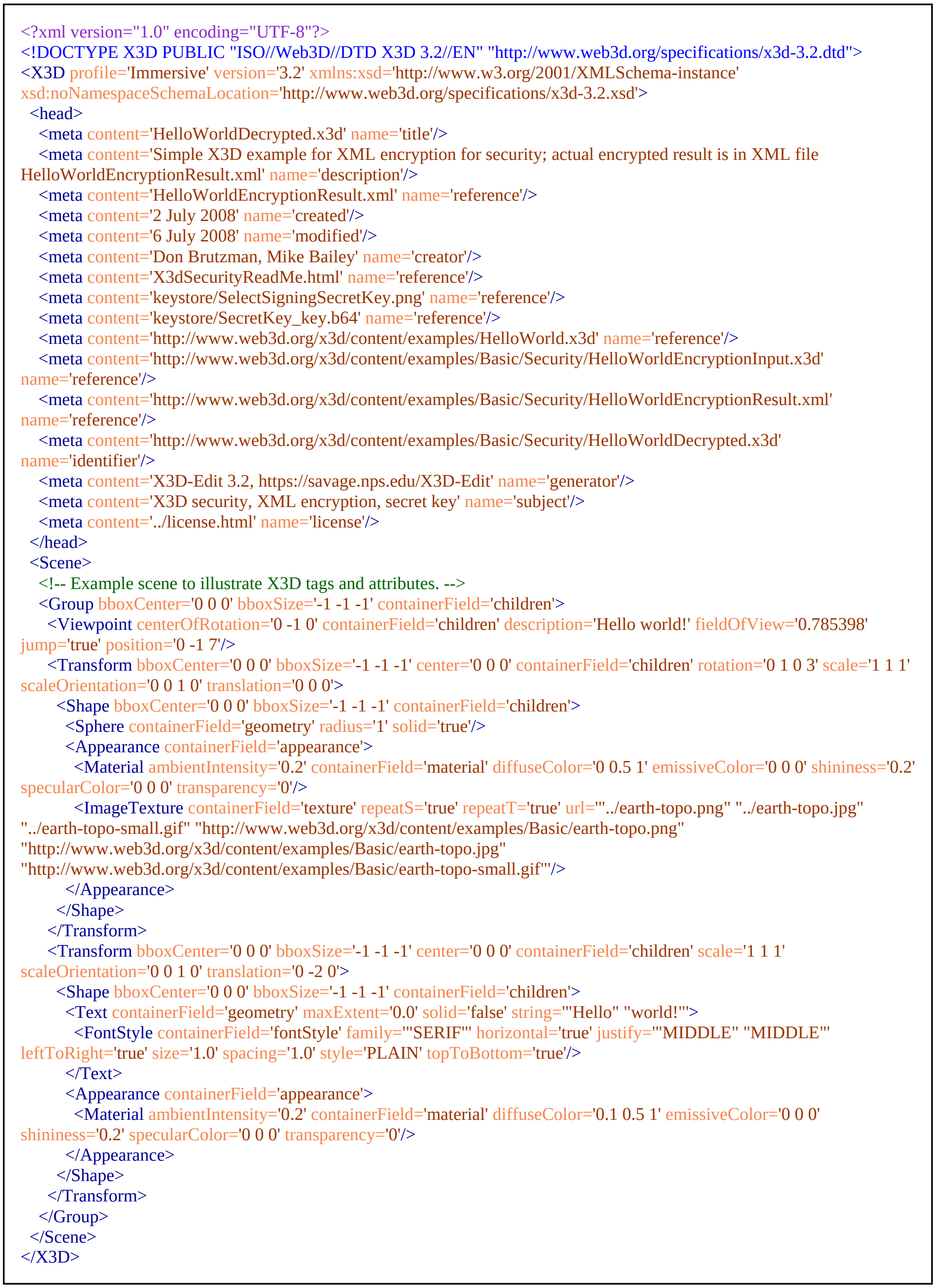
The X3D Security Examples show how to use the World Wide Web Consortium (W3C) Security Recommendations for XML Signature and XML Encryption with X3D.

Page	Description
Hello World Decrypted	Simple X3D example for XML encryption for security; actual encrypted result is in XML file HelloWorldEncryptionResult.xml
Hello World Encryption Input	Simple X3D example for XML encryption for security; actual encrypted result is in XML file HelloWorldEncryptionResult.xml
Hello World Signed	Simple X3D example with XML digital signature for author authentication, also used for example combined with encryption
Hello World Signed Decrypted	Simple X3D example with XML digital signature for author authentication, also used for example combined with encryption

http://www.web3d.org/x3d/content/examples/Basic/Security

Figure 67. An XML-based resource catalogue of results from various security operations is also available on the web3d.org site.

XML-based X3D data is reprepresented in Figures 68 through 71.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.2//EN" "http://www.web3d.org/specifications/x3d-3.2.dtd">
<X3D profile='Immersive' version='3.2' xmlns:xsd='http://www.w3.org/2001/XMLSchema-instance'
xsd:noNamespaceSchemaLocation='http://www.web3d.org/specifications/x3d-3.2.xsd'>
  <head>
    <meta content='HelloWorldDecrypted.x3d' name='title'/>
    <meta content='Simple X3D example for XML encryption for security; actual encrypted result is in XML file
HelloWorldEncryptionResult.xml' name='description'/>
    <meta content='HelloWorldEncryptionResult.xml' name='reference'/>
    <meta content='2 July 2008' name='created'/>
    <meta content='6 July 2008' name='modified'/>
    <meta content='Don Brutzman, Mike Bailey' name='creator'/>
    <meta content='X3dSecurityReadMe.html' name='reference'/>
    <meta content='keystore/SelectSigningSecretKey.png' name='reference'/>
    <meta content='keystore/SecretKey_key.b64' name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/HelloWorld.x3d' name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldEncryptionInput.x3d'
name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldEncryptionResult.xml'
name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldDecrypted.x3d'
name='identifier'/>
    <meta content='X3D-Edit 3.2, https://savage.nps.edu/X3D-Edit' name='generator'/>
    <meta content='X3D security, XML encryption, secret key' name='subject'/>
    <meta content='../license.html' name='license'/>
  </head>
  <Scene>
    <!-- Example scene to illustrate X3D tags and attributes. -->
    <Group bboxCenter='0 0 0' bboxSize='-1 -1 -1' containerField='children'>
      <Viewpoint centerOfRotation='0 -1 0' containerField='children' description='Hello world!' fieldOfView='0.785398'
jump='true' position='0 -1 7'/>
      <Transform bboxCenter='0 0 0' bboxSize='-1 -1 -1' center='0 0 0' containerField='children' rotation='0 1 0 3' scale='1 1 1'
scaleOrientation='0 0 1 0' translation='0 0 0'>
        <Shape bboxCenter='0 0 0' bboxSize='-1 -1 -1' containerField='children'>
          <Sphere containerField='geometry' radius='1' solid='true'/>
          <Appearance containerField='appearance'>
            <Material ambientIntensity='0.2' containerField='material' diffuseColor='0 0.5 1' emissiveColor='0 0 0' shininess='0.2'
specularColor='0 0 0' transparency='0'/>
            <ImageTexture containerField='texture' repeatS='true' repeatT='true' url='"../earth-topo.png" "../earth-topo.jpg"
"../earth-topo-small.gif" "http://www.web3d.org/x3d/content/examples/Basic/earth-topo.png"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo.jpg"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo-small.gif"'/>
          </Appearance>
        </Shape>
      </Transform>
      <Transform bboxCenter='0 0 0' bboxSize='-1 -1 -1' center='0 0 0' containerField='children' scale='1 1 1'
scaleOrientation='0 0 1 0' translation='0 -2 0'>
        <Shape bboxCenter='0 0 0' bboxSize='-1 -1 -1' containerField='children'>
          <Text containerField='geometry' maxExtent='0.0' solid='false' string='"Hello" "world!"'>
            <FontStyle containerField='fontStyle' family='"SERIF"' horizontal='true' justify='"MIDDLE" "MIDDLE"'
leftToRight='true' size='1.0' spacing='1.0' style='PLAIN' topToBottom='true'/>
          </Text>
          <Appearance containerField='appearance'>
            <Material ambientIntensity='0.2' containerField='material' diffuseColor='0.1 0.5 1' emissiveColor='0 0 0'
shininess='0.2' specularColor='0 0 0' transparency='0'/>
          </Appearance>
        </Shape>
      </Transform>
    </Group>
  </Scene>
</X3D>
```

Figure 68. HelloworldDecrypted illustrates the XML-based X3D data that is illustrated visually as a globe, which is seen in Figure 16

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.2//EN" "http://www.web3d.org/specifications/x3d-3.2.dtd">
<X3D profile='Immersive' version='3.2' xmlns:xsd='http://www.w3.org/2001/XMLSchema-instance'
xsd:noNamespaceSchemaLocation='http://www.web3d.org/specifications/x3d-3.2.xsd'>
  <head>
    <meta content='HelloWorldEncryptionInput.x3d' name='title'/>
    <meta content='Simple X3D example for XML encryption for security; actual encrypted result is in XML file
HelloWorldEncryptionResult.xml' name='description'/>
    <meta content='HelloWorldEncryptionResult.xml' name='reference'/>
    <meta content='2 July 2008' name='created'/>
    <meta content='6 July 2008' name='modified'/>
    <meta content='Don Brutzman, Mike Bailey' name='creator'/>
    <meta content='X3dSecurityReadMe.html' name='reference'/>
    <meta content='keystore/SelectSigningSecretKey.png' name='reference'/>
    <meta content='keystore/SecretKey_key.b64' name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/HelloWorld.x3d' name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldDecrypted.x3d'
name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldEncryptionResult.xml'
name='reference'/>
    <meta content='http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldEncryptionInput.x3d'
name='identifier'/>
    <meta content='X3D-Edit 3.2, https://savage.nps.edu/X3D-Edit' name='generator'/>
    <meta content='X3D security, XML encryption, secret key' name='subject'/>
    <meta content='../license.html' name='license'/>
  </head>
  <Scene>
    <!-- Example scene to illustrate X3D tags and attributes. -->
    <Group>
      <Viewpoint centerOfRotation='0 -1 0' description='Hello world!' position='0 -1 7'/>
      <Transform rotation='0 1 0 3'>
        <Shape>
          <Sphere/>
          <Appearance>
            <Material diffuseColor='0 0.5 1'/>
            <ImageTexture url='"../earth-topo.png" "../earth-topo.jpg" "../earth-topo-small.gif"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo.png"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo.jpg"
"http://www.web3d.org/x3d/content/examples/Basic/earth-topo-small.gif"'/>
          </Appearance>
        </Shape>
      </Transform>
      <Transform translation='0 -2 0'>
        <Shape>
          <Text solid='false' string='"Hello" "world!"'>
            <FontStyle justify='"MIDDLE" "MIDDLE"'/>
          </Text>
          <Appearance>
            <Material diffuseColor='0.1 0.5 1'/>
          </Appearance>
        </Shape>
      </Transform>
    </Group>
  </Scene>
</X3D>
```

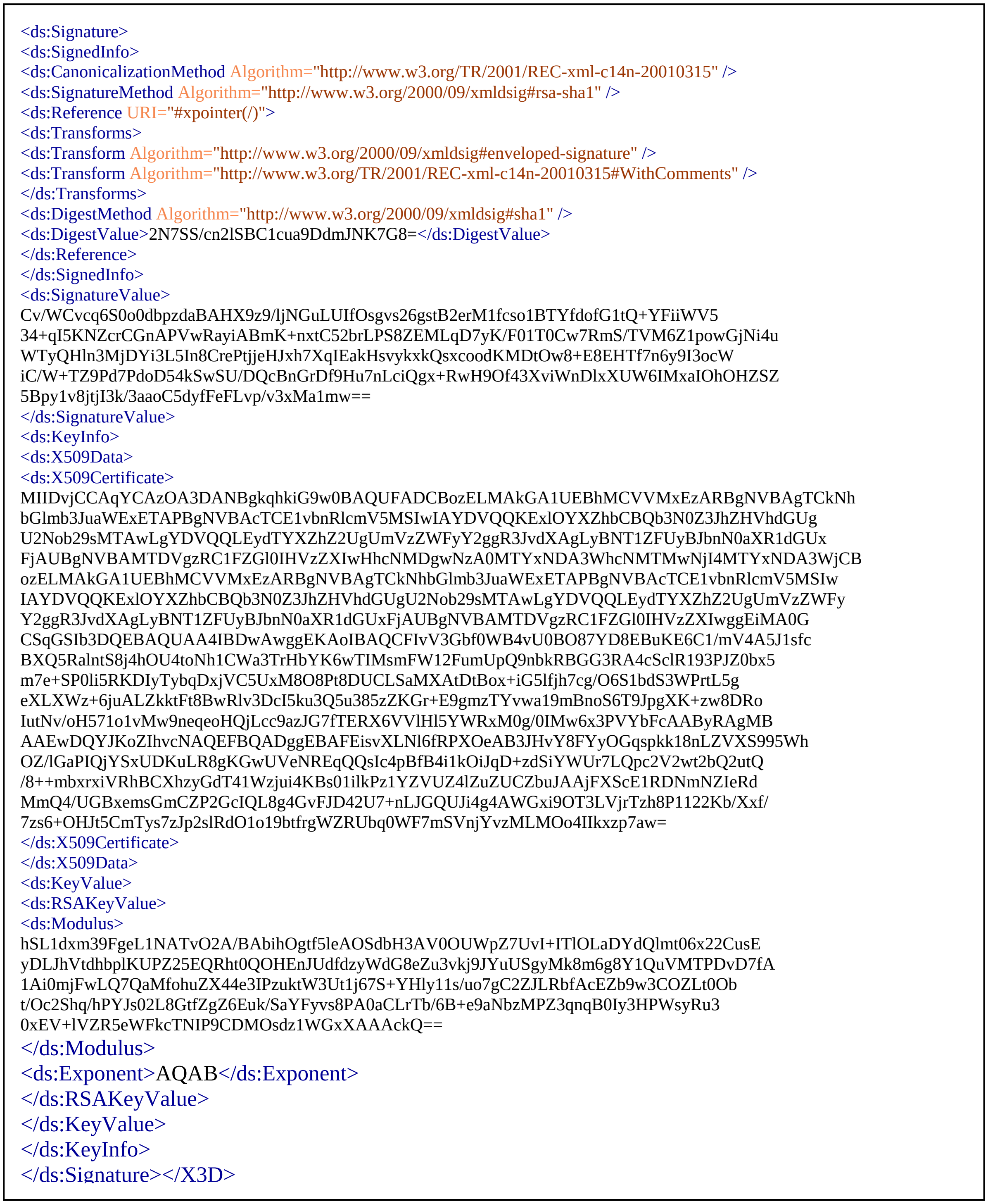
Figure 69. HelloWorldEncryptionInput illustrates the XML-based X3D data used prior to undergoing an XML Encryption operation.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.2//EN" "http://www.web3d.org/specifications/x3d-3.2.dtd">
<X3D xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance"
profile="Immersive" version="3.2" xsd:noNamespaceSchemaLocation="http://www.web3d.org/specifications/x3d-3.2.xsd">
 <head>
  <meta content="HelloWorldSigned.x3d" name="title" />
  <meta content="Simple X3D example with XML digital signature for author authentication, also used for example combined
with encryption" name="description" />
  <meta content="2 July 2008" name="created" />
  <meta content="6 July 2008" name="modified" />
  <meta content="Don Brutzman, Mike Bailey" name="creator" />
  <meta content="X3dSecurityReadMe.html" name="reference" />
  <meta content="keystore/SelectSigningKeyPair.png" name="reference" />
  <meta content="keystore/PublicPrivatePair_certificateChain.cer" name="reference" />
  <meta content="http://www.web3d.org/x3d/content/examples/HelloWorld.x3d" name="reference" />
  <meta content="http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldSignedEncryptedResult.xml"
name="reference" />
  <meta content="http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldSignedDecrypted.x3d"
name="reference" />
  <meta content="http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldSigned.x3d" name="identifier" />
  <meta content="X3D-Edit 3.2, https://savage.nps.edu/X3D-Edit" name="generator" />
  <meta content="../license.html" name="license" />
  <meta content="X3D security, XML signature authentication, public private key pair, XML encryption, secret key"
name="subject" />
 </head>
 <Scene>
  <!-- Example scene to illustrate X3D tags and attributes. -->
  <Group bboxCenter="0 0 0" bboxSize="-1 -1 -1" containerField="children">
   <Viewpoint centerOfRotation="0 -1 0" containerField="children" description="Hello world!" fieldOfView="0.785398"
jump="true" orientation="0 0 1 0" position="0 -1 7" />
   <Transform bboxCenter="0 0 0" bboxSize="-1 -1 -1" center="0 0 0" containerField="children" rotation="0 1 0 3" scale="1 1
1" scaleOrientation="0 0 1 0" translation="0 0 0">
    <Shape bboxCenter="0 0 0" bboxSize="-1 -1 -1" containerField="children">
     <Sphere containerField="geometry" radius="1" solid="true" />
     <Appearance containerField="appearance">
      <Material ambientIntensity="0.2" containerField="material" diffuseColor="0 0.5 1" emissiveColor="0 0 0"
shininess="0.2" specularColor="0 0 0" transparency="0" />
      <ImageTexture containerField="texture" repeatS="true" repeatT="true" url="&quot;../earth-topo.png&quot; &quot;../earth-
topo.jpg&quot; &quot;../earth-topo-small.gif&quot; &quot;http://www.web3d.org/x3d/content/examples/Basic/earth-
topo.png&quot; &quot;http://www.web3d.org/x3d/content/examples/Basic/earth-topo.jpg&quot;
&quot;http://www.web3d.org/x3d/content/examples/Basic/earth-topo-small.gif&quot;" />
     </Appearance>
    </Shape>
   </Transform>
   <Transform bboxCenter="0 0 0" bboxSize="-1 -1 -1" center="0 0 0" containerField="children" rotation="0 0 1 0" scale="1 1
1" scaleOrientation="0 0 1 0" translation="0 -2 0">
    <Shape bboxCenter="0 0 0" bboxSize="-1 -1 -1" containerField="children">
     <Text containerField="geometry" maxExtent="0.0" solid="false" string="&quot;Hello&quot; &quot;world!&quot;">
      <FontStyle containerField="fontStyle" family="&quot;SERIF&quot;" horizontal="true" justify="&quot;MIDDLE&quot;
&quot;MIDDLE&quot;" leftToRight="true" size="1.0" spacing="1.0" style="PLAIN" topToBottom="true" />
     </Text>
     <Appearance containerField="appearance">
      <Material ambientIntensity="0.2" containerField="material" diffuseColor="0.1 0.5 1" emissiveColor="0 0 0"
shininess="0.2" specularColor="0 0 0" transparency="0" />
     </Appearance>
    </Shape>
   </Transform>
  </Group>
 </Scene>
<ds:Signature>
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference URI="#xpointer(/)">
<ds:Transforms>
```

```xml
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>nqV+sWdljdElfGSBXbMMjBZyUfs=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
T9q7zV6KZUfyAg3gGTpKkAYWtY0QZxy8JWm/T6SI8eH7mrfCADeco5heVyXmTdTScVokSL1KFp2O
f96puB6Bo0BHG03AczpoxaBtcv1s8LvVBOukLXleKhpjrZ3vCuL2IyYP147KhKrXgRJMDfnYn7yp
xstPVWPtnzuIbt6DeMH/GQrJYKIvI4Hoj7Y0Y2Jl1UyGrHf0zICyVGOfPivbKRxOMScyk/UWZE0Q
tTLdsYM5tBrGVwZqf5ZXQKutS/nl7V/GnMPRtcRiqU63E9AVwfcR1UJu/XV/ZdEChGDSKke4RCjA
SnN3XtG9wE+fWfuldJ/mG1wUa1lBDfj/Em1aaQ==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIDvjCCAqYCAzOA3DANBgkqhkiG9w0BAQUFADCBozELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExETAPBgNVBAcTCE1vbnRlcmV5MSIwIAYDVQQKExlOYXZhbCBQb3N0Z3JhZHVhdGUg
U2Nob29sMTAwLgYDVQQLEydTYXZhZ2UgUmVzZWFyY2ggR3JvdXAgLyBNT1ZFUyBJbnN0aXR1dGUx
FjAUBgNVBAMTDVgzRC1FZGl0IHVzZXIwHhcNMDgwNzA0MTYxNDA3WhcNMTMwNjI4MTYxNDA3WjCB
ozELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCE1vbnRlcmV5MSIw
IAYDVQQKExlOYXZhbCBQb3N0Z3JhZHVhdGUgU2Nob29sMTAwLgYDVQQLEydTYXZhZ2UgUmVzZWFy
Y2ggR3JvdXAgLyBNT1ZFUyBJbnN0aXR1dGUxFjAUBgNVBAMTDVgzRC1FZGl0IHVzZXIwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCFIvV3Gbf0WB4vU0BO87YD8EBuKE6C1/mV4A5J1sfc
BXQ5RalntS8j4hOU4toNh1CWa3TrHbYK6wTIMsmFW12FumUpQ9nbkRBGG3RA4cSclR193PJZ0bx5
m7e+SP0li5RKDIyTybqDxjVC5UxM8O8Pt8DUCLSaMXAtDtBox+iG5lfjh7cg/O6S1bdS3WPrtL5g
eXLXWz+6juALZkktFt8BwRlv3DcI5ku3Q5u385zZKGr+E9gmzTYvwa19mBnoS6T9JpgXK+zw8DRo
IutNv/oH571o1vMw9neqeoHQjLcc9azJG7fTERX6VVlHl5YWRxM0g/0IMw6x3PVYbFcAAByRAgMB
AAEwDQYJKoZIhvcNAQEFBQADggEBAFEisvXLNl6fRPXOeAB3JHvY8FYyOGqspkk18nLZVXS995Wh
OZ/lGaPIQjYSxUDKuLR8gKGwUVeNREqQQsIc4pBfB4i1kOiJqD+zdSiYWUr7LQpc2V2wt2bQ2utQ
/8++mbxrxiVRhBCXhzyGdT41Wzjui4KBs01ilkPz1YZVUZ4lZuZUCZbuJAAjFXScE1RDNmNZIeRd
MmQ4/UGBxemsGmCZP2GcIQL8g4GvFJD42U7+nLJGQUJi4g4AWGxi9OT3LVjrTzh8P1122Kb/Xxf/
7zs6+OHJt5CmTys7zJp2slRdO1o19btfrgWZRUbq0WF7mSVnjYvzMLMOo4IIkxzp7aw=
</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
hSL1dxm39FgeL1NATvO2A/BAbihOgtf5leAOSdbH3AV0OUWpZ7UvI+ITlOLaDYdQlmt06x22CusE
yDLJhVtdhbplKUPZ25EQRht0QOHEnJUdfdzyWdG8eZu3vkj9JYuUSgyMk8m6g8Y1QuVMTPDvD7fA
1Ai0mjFwLQ7QaMfohuZX44e3IPzuktW3Ut1j67S+YHly11s/uo7gC2ZJLRbfAcEZb9w3COZLt0Ob
t/Oc2Shq/hPYJs02L8GtfZgZ6Euk/SaYFyvs8PA0aCLrTb/6B+e9aNbzMPZ3qnqB0Iy3HPWsyRu3
0xEV+lVZR5eWFkcTNIP9CDMOsdz1WGxXAAAckQ==
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature></X3D>
```

Figure 70. HelloWorldSigned illustrates the XML-based X3D data used after an XML Digital Signature operation.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X3D PUBLIC "ISO//Web3D//DTD X3D 3.2//EN" "http://www.web3d.org/specifications/x3d-3.2.dtd">
<X3D xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance"
profile="Immersive" version="3.2" xsd:noNamespaceSchemaLocation="http://www.web3d.org/specifications/x3d-3.2.xsd">
 <head>
  <meta content="HelloWorldSignedDecrypted.x3d" name="title" />
  <meta content="Simple X3D example with XML digital signature for author authentication, also used for example
combined with encryption" name="description" />
  <meta content="2 July 2008" name="created" />
  <meta content="6 July 2008" name="modified" />
  <meta content="Don Brutzman, Mike Bailey" name="creator" />
  <meta content="X3dSecurityReadMe.html" name="reference" />
  <meta content="keystore/SelectSigningKeyPair.png" name="reference" />
  <meta content="keystore/PublicPrivatePair_certificateChain.cer" name="reference" />
  <meta content="http://www.web3d.org/x3d/content/examples/HelloWorld.x3d" name="reference" />
  <meta content="http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldSignedEncryptedResult.xml"
name="reference" />
  <meta content="http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldSigned.x3d" name="reference"
/>
  <meta content="http://www.web3d.org/x3d/content/examples/Basic/Security/HelloWorldSignedDecrypted.x3d"
name="identifier" />
  <meta content="X3D-Edit 3.2, https://savage.nps.edu/X3D-Edit" name="generator" />
  <meta content="../license.html" name="license" />
  <meta content="X3D security, XML signature authentication, public private key pair, XML encryption, secret key"
name="subject" />
 </head>
 <Scene>
  <!-- Example scene to illustrate X3D tags and attributes. -->
  <Group bboxCenter="0 0 0" bboxSize="-1 -1 -1" containerField="children">
   <Viewpoint centerOfRotation="0 -1 0" containerField="children" description="Hello world!" fieldOfView="0.785398"
jump="true" orientation="0 0 1 0" position="0 -1 7" />
   <Transform bboxCenter="0 0 0" bboxSize="-1 -1 -1" center="0 0 0" containerField="children" rotation="0 1 0 3"
scale="1 1 1" scaleOrientation="0 0 1 0" translation="0 0 0">
    <Shape bboxCenter="0 0 0" bboxSize="-1 -1 -1" containerField="children">
     <Sphere containerField="geometry" radius="1" solid="true" />
     <Appearance containerField="appearance">
      <Material ambientIntensity="0.2" containerField="material" diffuseColor="0 0.5 1" emissiveColor="0 0 0"
shininess="0.2" specularColor="0 0 0" transparency="0" />
      <ImageTexture containerField="texture" repeatS="true" repeatT="true" url="&quot;../earth-topo.png&quot;
&quot;../earth-topo.jpg&quot; &quot;../earth-topo-small.gif&quot;
&quot;http://www.web3d.org/x3d/content/examples/Basic/earth-topo.png&quot;
&quot;http://www.web3d.org/x3d/content/examples/Basic/earth-topo.jpg&quot;
&quot;http://www.web3d.org/x3d/content/examples/Basic/earth-topo-small.gif&quot;" />
     </Appearance>
    </Shape>
   </Transform>
   <Transform bboxCenter="0 0 0" bboxSize="-1 -1 -1" center="0 0 0" containerField="children" rotation="0 0 1 0"
scale="1 1 1" scaleOrientation="0 0 1 0" translation="0 -2 0">
    <Shape bboxCenter="0 0 0" bboxSize="-1 -1 -1" containerField="children">
     <Text containerField="geometry" maxExtent="0.0" solid="false" string="&quot;Hello&quot; &quot;world!&quot;">
      <FontStyle containerField="fontStyle" family="&quot;SERIF&quot;" horizontal="true"
justify="&quot;MIDDLE&quot; &quot;MIDDLE&quot;" leftToRight="true" size="1.0" spacing="1.0" style="PLAIN"
topToBottom="true" />
     </Text>
<Appearance containerField="appearance">
      <Material ambientIntensity="0.2" containerField="material" diffuseColor="0.1 0.5 1" emissiveColor="0 0 0"
shininess="0.2" specularColor="0 0 0" transparency="0" />
     </Appearance>
    </Shape>
   </Transform>
  </Group>
</Scene>
```



```xml
<ds:Signature>
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference URI="#xpointer(/)">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>2N7SS/cn2lSBC1cua9DdmJNK7G8=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
Cv/WCvcq6S0o0dbpzdaBAHX9z9/ljNGuLUIfOsgvs26gstB2erM1fcso1BTYfdofG1tQ+YFiiWV5
34+qI5KNZcrCGnAPVwRayiABmK+nxtC52brLPS8ZEMLqD7yK/F01T0Cw7RmS/TVM6Z1powGjNi4u
WTyQHln3MjDYi3L5In8CrePtjjeHJxh7XqIEakHsvykxkQsxcoodKMDtOw8+E8EHTf7n6y9I3ocW
iC/W+TZ9Pd7PdoD54kSwSU/DQcBnGrDf9Hu7nLciQgx+RwH9Of43XviWnDlxXUW6IMxaIOhOHZSZ
5Bpy1v8jtjI3k/3aaoC5dyfFeFLvp/v3xMa1mw==
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIDvjCCAqYCAzOA3DANBgkqhkiG9w0BAQUFADCBozELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExETAPBgNVBAcTCE1vbnRlcmV5MSIwIAYDVQQKExlOYXZhbCBQb3N0Z3JhZHVhdGUg
U2Nob29sMTAwLgYDVQQLEydTYXZhZ2UgUmVzZWFyY2ggR3JvdXAgLyBNT1ZFUyBJbnN0aXR1dGUx
FjAUBgNVBAMTDVgzRC1FZGl0IHVzZXIwHhcNMDgwNzA0MTYxNDA3WhcNMTMwNjI4MTYxNDA3WjCB
ozELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCE1vbnRlcmV5MSIw
IAYDVQQKExlOYXZhbCBQb3N0Z3JhZHVhdGUgU2Nob29sMTAwLgYDVQQLEydTYXZhZ2UgUmVzZWFy
Y2ggR3JvdXAgLyBNT1ZFUyBJbnN0aXR1dGUxFjAUBgNVBAMTDVgzRC1FZGl0IHVzZXIwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCFIvV3Gbf0WB4vU0BO87YD8EBuKE6C1/mV4A5J1sfc
BXQ5RalntS8j4hOU4toNh1CWa3TrHbYK6wTIMsmFW12FumUpQ9nbkRBGG3RA4cSclR193PJZ0bx5
m7e+SP0li5RKDIyTybqDxjVC5UxM8O8Pt8DUCLSaMXAtDtBox+iG5lfjh7cg/O6S1bdS3WPrtL5g
eXLXWz+6juALZkktFt8BwRlv3DcI5ku3Q5u385zZKGr+E9gmzTYvwa19mBnoS6T9JpgXK+zw8DRo
IutNv/oH571o1vMw9neqeoHQjLcc9azJG7fTERX6VVlHl5YWRxM0g/0IMw6x3PVYbFcAAByRAgMB
AAEwDQYJKoZIhvcNAQEFBQADggEBAFEisvXLNl6fRPXOeAB3JHvY8FYyOGqspkk18nLZVXS995Wh
OZ/lGaPIQjYSxUDKuLR8gKGwUVeNREqQQsIc4pBfB4i1kOiJqD+zdSiYWUr7LQpc2V2wt2bQ2utQ
/8++mbxrxiVRhBCXhzyGdT41Wzjui4KBs01ilkPz1YZVUZ4lZuZUCZbuJAAjFXScE1RDNmNZIeRd
MmQ4/UGBxemsGmCZP2GcIQL8g4GvFJD42U7+nLJGQUJi4g4AWGxi9OT3LVjrTzh8P1122Kb/Xxf/
7zs6+OHJt5CmTys7zJp2slRdO1o19btfrgWZRUbq0WF7mSVnjYvzMLMOo4IIkxzp7aw=
</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
hSL1dxm39FgeL1NATvO2A/BAbihOgtf5leAOSdbH3AV0OUWpZ7UvI+ITlOLaDYdQlmt06x22CusE
yDLJhVtdhbplKUPZ25EQRht0QOHEnJUdfdzyWdG8eZu3vkj9JYuUSgyMk8m6g8Y1QuVMTPDvD7fA
1Ai0mjFwLQ7QaMfohuZX44e3IPzuktW3Ut1j67S+YHly11s/uo7gC2ZJLRbfAcEZb9w3COZLt0Ob
t/Oc2Shq/hPYJs02L8GtfZgZ6Euk/SaYFyvs8PA0aCLrTb/6B+e9aNbzMPZ3qnqB0Iy3HPWsyRu3
0xEV+lVZR5eWFkcTNIP9CDMOsdz1WGxXAAAckQ==
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature></X3D>
```

Figure 71. HelloWorldSigned illustrates the XML-based X3D data used after an XML Digital Signature operation.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ayers, Danny, et al. (2007). *Beginning XML 4th Edition* Wiley Publishing, Inc.

Abadi, Martin, et al.. "A Logic of Authentication" ACM Transactions on Computer Systems, Vol. 8, No. 1, February 1990.

Adams, Carlisle, et al. (2001). "Introduction to XML Digital Signatures" Retrieved January 2009 from http://www.xml.com/pub/a/2001/08/08/xmldsig.html.

Alesso, H. P., et al. *Developing Semantic Web Services* A.K. Peters, Ltd., 2005.

Altova. "XML Editor, Data Management, UML and Web Services Tools," Retrieved August 2009 from http://www.altova.com.

Bartel, Mark, et al. (2008) "XML Signature Syntax and Processing (Second Edition) W3C Recommendation 10 June 2008" Retreived September 2008 from http://www.w3.org/TR/xmldsig-core. The Internet Society & W3C.

Benaïssa, Nazim. "Modelling Attaker's Knowledge for Cascade Cryptographic Protocols" Retrieved August 2009 from http://www.springerlink.com/content/05n6782733q123g3/fulltext.pdf

Berners-Lee, Tim (1999). *Weaving the Web, The Past, Present and Future of the World Wide Web by its inventor*, Orion Business Books.

Blais, Curtis et al."DIS-XML An XML Representation of Distributed Interactive Simulation Protocol Data Units @ 2006", Retrieved August 2009 from http://www.sisostds.org/index.

Bos, Bert. "XML in 10 Points", Retrieved August 2009 from http://www.w3.org/XML/1999/XML-in10-points-19990327.

Boyer, John. "Canonical XML 1.0 W3C Recommendation 15 March 2001", IETF/W3C XML Signature Working Group Retrieved March 2009 from http://www.w3.org/TR/2001/REC-xml-c14n-20010315.

Bray, Tim, et al. XML Core Working Group (2008), "Extensible Markup Language (XML) 1.0 (Fifth Edition) W3C Recommendation 26 November 2008", Retrieved April 2009 from http://www.w3.org/TR/xml/#sec-well-formed.

Brutzman, Don, et al. "X3D-Edit Authoring Tool for Extensible 3D (X3D) Graphics" Retrieved August 2009 from https://savage.nps.edu/X3D-Edit.

Brutzman, Don, et al. Basic Security Examples, Retrieved January 2009 from http://www.web3d.org/x3d/content/examples/Basic/Security

Bush, George W. (2004). "Executive Order 13356 of August 27, 2004–Strengthening the Sharing of Terrorism Information to Protect Americans" Federal Register Vol. 69 No. 169 Sept 2004 Retrieved August 2009 from http://www.archives.gov/federal-register/executive-orders/2004.html.

Bush, George W. (2005). "Executive Order 13388 of October 25, 2005–Further Strengthening the Sharing of Terrorism Information to Protect Americans", Federal Register Vol. 70 No. 207 Retrieved August 2009 from http://www.archives.gov/federal-register/executive-orders/2005.html.

Bush, George W. (2005) "Executive Order 13392 of December 14, 2005–Improving Agency Disclosure of Information" Federal Register Vol. 70 No. 242 Retrieved August 2005 from http://www.archives.gov/federal-register/executive-orders/2005.html.

Center for Advanced Defense Studies. Retrieved August 2009 from http://www.c4ads.org/projects

Center for Strategic and International Studies (2008). "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th presidency" Retreived February 2009 from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

CISCO. "CISCO IOS IPsec" Retrieved August 2009 from http://www.cisco.com/en/US/products/ps6635/products_ios_protocol_group_home.html.

CNSS Glossary Working Group. "National Information Assurance (IA) Glossary CNSS Instruction No. 4009", Retrieved June 2009 from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

Combs, Gerald. WireShark/Ethereal, Retrieved August 2009 from http://www.wireshark.com.

Department of Defense (2003). "Command, Control, Communications, Computers, and Intelligence (C4I) Joint Extensible Markup Language (XML) Message Text Format (MTF) Roadmap (JXMR)" Retrieved August 2009 from https://metadata.dod.mil/mdr/download.htm?contentItemId=urn:uuid:e917c5ae-a0bf-48da-8770-fafaefceb75e.

Department of Defense. "Information Assurance Implementation", Retrieved February 2009 from http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.

Department of Defense. “Information Assurance in Defense Acquisition Systems” Retrieved February 2009 from “http://www.marcorsyscom.usmc.mil/sites/ia/documents/i85801p.pdf .

Dillaway, Blair et al. (2002). “XML Encryption Syntax and Processing W3C Recommendation 10 December 2002”, Retrieved August 2009 from http://www.w3.org/TR/xmlenc-core

Dinolt, George (2009). “Dolev Yao Model of the Intruder Lecture Notes” CS4615 Protocol Analysis Lecture Notes, Retreived April 2009 from https://cle.nps.edu.

Dinolt, George (2009). “Strand Space Analysis of Needham-Schroeder-Lowe Lecture Notes”, CS4615 Protocol Analysis, Retreived May 2009 from https://cle.nps.edu.

Dolev D., and Yoa, A.C (1983). “On the Security of Public Key Protocols” IEEE transactions on Information Theory 29(2):198-208.

Elector Electronics World Wide. “Mobile Phone Sniffer issue 310 May 2002,” http://www.elektor.com/magazines/2002/may/mobile-phone-sniffer.55700.lynkx , Retrieved June 2009.

Efficient XML Interchange (EXI) Working Group (2008). “Efficient XML Interchange (EXI) Format 1.0 W3C Working Draft 19 September 2008”, W3C Retrieved July 2009 from http://www.w3.org/TR/2008/WD-exi-20080919

Encarta Encyclopedia. “piracy”, Retrieved August 2009 from http://encarta.msn.com/encnet/refpages/searchdetail.aspx?q=piracy&pg=1&grp=ans

Fabrega, Javier et al. (1999). “Strand Spaces: Proving Security Protocols Correct*,” Journal of Computer Security.

Federal Trade Commission and Department of Commerce (2001). “Electronic Signatures in Global and National Commerce Act The Consumer Consent Provision in Section 101(c)(1)(C)(ii)”, Retrieved March 2009 from http://www.ftc.gov/os/2001/06/esign7.htm.

Geroimenko, Vladimir et al. (2005). *Visualizing Information Using SVG and X3D: XML-based Technologies for the XML-Based Web*, Springer-Verlag London Limited, Singapore.

Hallam-Baker et al. “XML Key Management Specification (XKMS)”, http://www10.org/cdrom/posters/1129.pdf Retrieved August 2009.

Hallam-Baker, Phillip (2007). *The DotCrime Manifesto: How to Stop Internet Crime*, Addison-Wesley.

Harris, Shon (2007). *All-in-one CISSP Exam Guide, 4th Edition* Mcgraw Hill-Osborne Media.

Hill, Brad. "A Taxonomy of Attacks against XML Digital Signatures & Encryption" Retreived August 2009 from http://www.isecpartners.com/files/iSEC_HILL_AttackingXMLSecurity_Handout.pdf.

Hwang, Min Shiang et al. (2004). "A Key Authentication Scheme with Non-Repudiation", ACM SIGOPS Operating Systems Review, Volume 38, Issue 3 Jennings, Frank et al, "Securing XML Documents", Retrieved June 2009 from http://www.packtpub.com/article/securing-xml-documents.

IETF/W3C XML Signature Working Group. "Canonical XML Version 1.0 W3C Recommendation 15 March 2001", Retrieved July 2009 from http://www.w3.org/TR/xml-c14n.html.

Joint Interoperability Test Command. "Coalition Warrior Interoperability Demonstration 2007 Report: Coalition Secure Management and Operations System (COSMOS)" Retreived August 2009 from http://www.cwid.js.mil/public/CWID07FR/htmlfiles/314

Kangasharju, Jaakko (2007). "Efficient Implementation of XML Security for Mobile Devices" Computer Society 2007 IEEE International Conference on Web Services.

Kangasharju, Jaakko. "Efficient XML Interchange (EXI) Impacts", Retrieved June 2009 from http://www.w3.org/TR/exi-impacts,

Kay, Michael. "Up-conversion using XSLT 2.0", Retrieved July 2009 from http://www.saxonica.com/papers/ideadb-1.1/mhk-paper.xml.

Langevin, et al. (2008). "Securing Cyberspace for the 44th Presidency", Center for Strategic and International Studies.

Nair, Smitha S. "XML Compression Techniques: A Survey", Retrieved June 2007 from http://people.ok.ubc.ca/rlawrenc/research/Students/SN_04_XMLCompress.pdf,

National Computer Security Center. "A Guide to Understanding Discretionary Access Control in Trusted Systems" Retrieved February 2009 from http://www.fas.org/irp/nsa/rainbow/tg003.htm.

National Institute of Standards and Technology Manufacturing Systems Integration Div. "MSID XML Testbed" Retrieved May 2009 from http://www.mel.nist.gov/msid/XML_testbed/common_terms.html.

PCI Security Standards Council. “Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms Version 1.2 October 2008”, Retrieved June 2009 from https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf.

Pokek, Gerald J., et al. (1974). “Formal requirements for virtualizable third generation architectures” Communications of the ACM, Vol 17 , Issue 7.

Proceedings. “The Commanders Respond Issue March 2009, Vol 135/3/1273”, Retrieved March 2009 from http://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1808

Rawlings, Michael C. (2004). “Using XML with Legacy Business Applications” Retrieved August 2009 from http://books.google.com

Reliefweb Office for the Coordination of Humanitarian Affairs. HOA.jpg Retrieved August 2009 from http://www.reliefweb.int/mapc/afr_ne/hornofafrica.jpg.

Sakr, Sherif (2009). “XML compression techniques: A survey and comparison” Journal of Computer and System Sciences Volume 75 Issue 5 Pp. 303 – 322.

Schneier, Bruce (1996). *Applied Cryptography Second Edition Protocols, Algorithms, and Source Code in C*, John Wiley & Sons.

Serin, E. “Design and Test of the Cross-Format Schema Protocol (XSFP) for Network Virtual Environments”, Master’s Thesis, Naval Postgraduate School, Monterey, CA, March 2003.

The Shmoo Group. “AirSnort HomePage”, Retreived June 2009 from http://airsnort.shmoo.com.

Siddiqui, Bilal. “Exploring XML Encryption, Part 1 Demonstrating the secure exchange of structured data” Retrieved May 2009 from http://www.ibm.com/developerworks/library/x-encrypt/index.html.

Snyder, Sheldon et al. “Efficient XML Interchange: Compact, Efficient, and Standards-Based XML for Modeling and Simulation” Naval Postgraduate School Modeling Virtual Environments and Simulations Institute Scenario Authoring and Visualization for Advanced Graphical Environments Labs@ 2009 Manuscript unpublished.

Sourceforge. “Network Protocols and Communications Utilities Under XMSF” Retrieved August 2009 from http://xmsf.sourceforge.net/XmsfComms.html.

Sourceforge.”XSBC:XML Schema-based Binary Compression” Retreived August 2009 from http://xmsf.sourceforge.net/xsbc.html.

Sullivan, Patrick. "Evaluating the Effectiveness of Waterside Security Alternatives for Force Protection of US Navy Ships and Installations using X3D Graphics and Agent Based Simulation," MOVES Master's Thesis, Naval Postgraduate School, September 2006.

SyncRO Soft Ltd. Oxygen XML Editor, Retrieved August 2009 from http://www.oxygenxml.com.

Trinity Atomic Website. " Radiation Exposures Whole Body over 15 rem", Retrieved August 2009 from http://www.cddc.vt.edu/host/atomic/accident/radexpos.html.

The Unicode Consortium. Retrieved August 2009 from http://unicode.org.

United Nations Convention on the Law of the Sea of 10 December 1982. "United Nations Convention on the Law of the Sea Agreement Relating to the Implementation of Part XI of the Convention", Retrieved March 2009 from http://www.un.org/Depts/los/convention_agreements/texts/unclos/closindx.htm

United States Code Title 14 Part 1 Chapter 5 Article 89a. Law Enforcement Retrieved June 2009 from http://www.law.cornell.edu/uscode/14/89.html.

United States Coast Guard. "Boat Crew Seamanship Manual COMDTINST M16114.5C Train, Maintain, Operate" Retrieved August 2009 from http://www.uscg.mil/directives/listing_cim.asp?id=16000-16999.

W3C. http://www.w3.org/XML Retreived August 2009.

W3C Semantic Web Activity. http://www.w3.org/2001/sw Retrieved August 2009.

W3C Schema XML Working Group."W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures W3C Candidate Recommendation 30 April 2009" Retrieved August 2009 from http://www.w3.org/TR/2009/CR-xmlschema11-1-20090430/#xsi-namespace.

W3C Working Group. "XML Encryption WG" Retrieved March 2009 from http://www.w3.org/Encryption/2001.

Web3D Consortium. Retrieved "What is X3D" August 2009 from http://www.web3D.org/about/overview

Web and XML Glossary. Retrieved August 2009 from http://dret.net/glossary/pkcs.

Williams, Lorraine C. (2002). "A Discussion of the Importance of Key Length in Symmetric and Asymmetric Cryptography" Retrieved August 2009 from http://www.giac.org/certified_professionals/practicals/gsec/0848.php.

Worthington, David. “Will EXI Mean XML Everywhere? Efficient XML accelerates the performance of XML and reduces its data representation” Retrieved August 2009 from http://www.sdtimes.com/content/article.aspx?ArticleID=31243.

XML Core Working Group. ”Extensible Markup Language 1.0 Fifth Edition W3C Recommendation 26 November 2008” Retreived from January 2009 from http://www.w3.org/TR/xml/#sec-well-formed.

XML Core Working Group.”Namespaces in XML 1.1 (Second Edition) W3C Recommendation 16 August 2006” Retrieved August 2009 from http://www.w3.org/TR/2006/REC-xml-names11-20060816.

XML Encryption Working Group. “XML Encryption Requirements W3C Note 04 Marcy 2002” Retrieved May 2009 from http://www.w3.org/TR/xml-encryption-req#ref-XML-DSIG.

XMPP Standards Foundation. Retrieved August 2009 from http://XMPP.org.

XSL Working Group.”XSL Transformation Version 2.0 W3C Recommendation 23 January 2007” Retrieved August 2009 from http://www.w3.org/TR/xslt20.

W3C XML Security Specifications Maintenance Working Group. “XML Signature Syntax and Processing (Second Edition) W3C Recommendation 10 June 2008”, Retrieved July 2009 from http://www.w3.org/TR/xmldsig-core.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Don Brutzman, Ph.D.
   Naval Postgraduate School
   Monterey, CA

4. Professor Mark J. Pullen
   George Mason University
   School of Information Technology and Engineering
   Fairfax VA

5. Janek Kaliczak, Vice President Research and Development
   Themis Vision Systems, LLC
   NASA Stennis Space Center,
   Mississippi

6. Gary Holness, PhD
   Lockheed Martin Advanced Technology Laboratories
   Lead Research Scientist
   Cherry Hill, NJ

7. Rev. Selena Williams
   Christ Temple Church of Personal Experience
   30 Kennilworth St
   Roxbury, MA

8. LCDR Jeffrey Scott Williams Sr
   NATO
   Brussels, Belgium

9. Brandon K. Thomas
   Marine Corps Warfighting Laboratory
   Experiment Division
   Quantico, VA

10. James Ehlert
Naval Postgraduate School
Monterey, CA

11. CAPT Jeffrey Kline, USN (Ret.)
Maritime Defense & Security Research Group
Operations Research Department
Naval Postgraduate School
Monterey, CA

12. Richard Lee
Office of the Secretary of Defense – Acquisition, Technology and Logistics
Washington, DC

13. Phillip Hallam-Baker
Boston, MA

14. Erik Chaum
Naval Undersea Warefare Center
Newport, RI

15. Naval Network Warfare Command
Norfolk, VA

16. Don McGregor
Naval Postgraduate School
Monterey, CA

17. Dr. Jim Eagle
Operations Research Department
Naval Postgraduate School
Monterey, CA

18. D.C. Boger
Naval Postgraduate School
Monterey, CA

19. Cynthia Irvine
Center for Information Security Research
Naval Postgraduate School
Monterey, CA

20. Donald Gaver
Naval Postgraduate School
Monterey, CA

21. NSWC Dam Neck
Virginia Beach, VA

22. LCDR Floyd Williams
VAW-125
Norfolk, VA

23. Chuck Kimzey
National Security Institute
Naval Postgraduate School
Monterey, CA

24. Thomas Roessler
Security Activity Lead; Acting T&S Domain Leader
World Wide Web Consortium
Cambridge, MA

25. Scenario Authoring and Visualization for Advanced Graphical Environments (SAVAGE)
Naval Postgraduate School
Monterey, CA

26. Rex Buddenberg
Naval Postgraduate School
Monterey, CA

27. Rick Hayes-Roth
Naval Postgraduate School
Monterey, CA

28. Gene Small
Embedded Systems Design
San Francisco, CA

29. James D. Neushul
MARCORSYSCOM
Quantico, VA